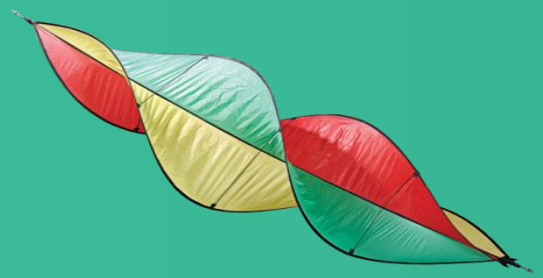
KU LEUVEN

TECHNOLOGIECAMPUS GENT



Android in Industrial Settings

Jan Vossaert & Vincent Raes

Veilige industriële netwerken

https://msec.be/verboten/

22/12/2016

Overview

- Secure Mobile Access to the Local ICS Network
  - General purpose devices
  - Mixed OT and IT functionality

- Secure Services on Embedded Android in Industrial Settings
  - Embedded devices
  - Dedicated OT functionality

KU LEUVEN

Secure Mobile Access to the Local ICS Network

KU LEUVEN

Introduction

- Use mobile devices in ICS environments
  - Hardware platform
  - Multi-purpose device
  - Built-in security & management technologies

Introduction

*"…**monitor** any area of production—packaging status, cook temperature or frying capacity—from the palm of their hands..."*
(Hillshire Brands)

*"We use the app to **monitor** our gas detection devices, but we also use a few controls in the app that allow us to **remotely silence the alarms**…"* (Bayer Corp. in Pittsburgh)

*"The main advantage of a mobile device in an industrial setting is the **real-time access to all information independent** of the workers **location**"*

*"We have a few in-house mobile applications for **handling work orders and purchase orders**, as well as preventative maintenance and inventory."*

*"troubleshoot **without** the help from the **control room**"*

*"A mobile HMI **reduces communication errors** between people by allowing the **field operator** to access the same data as the **control room** operator."*

*"…anytime **access to real-time and historical production data** and trends, operators can see where there are problems, where problems might potentially arise, or where additional capacity exists to increase production or run an alternative product."*
(Hillshire Brands)

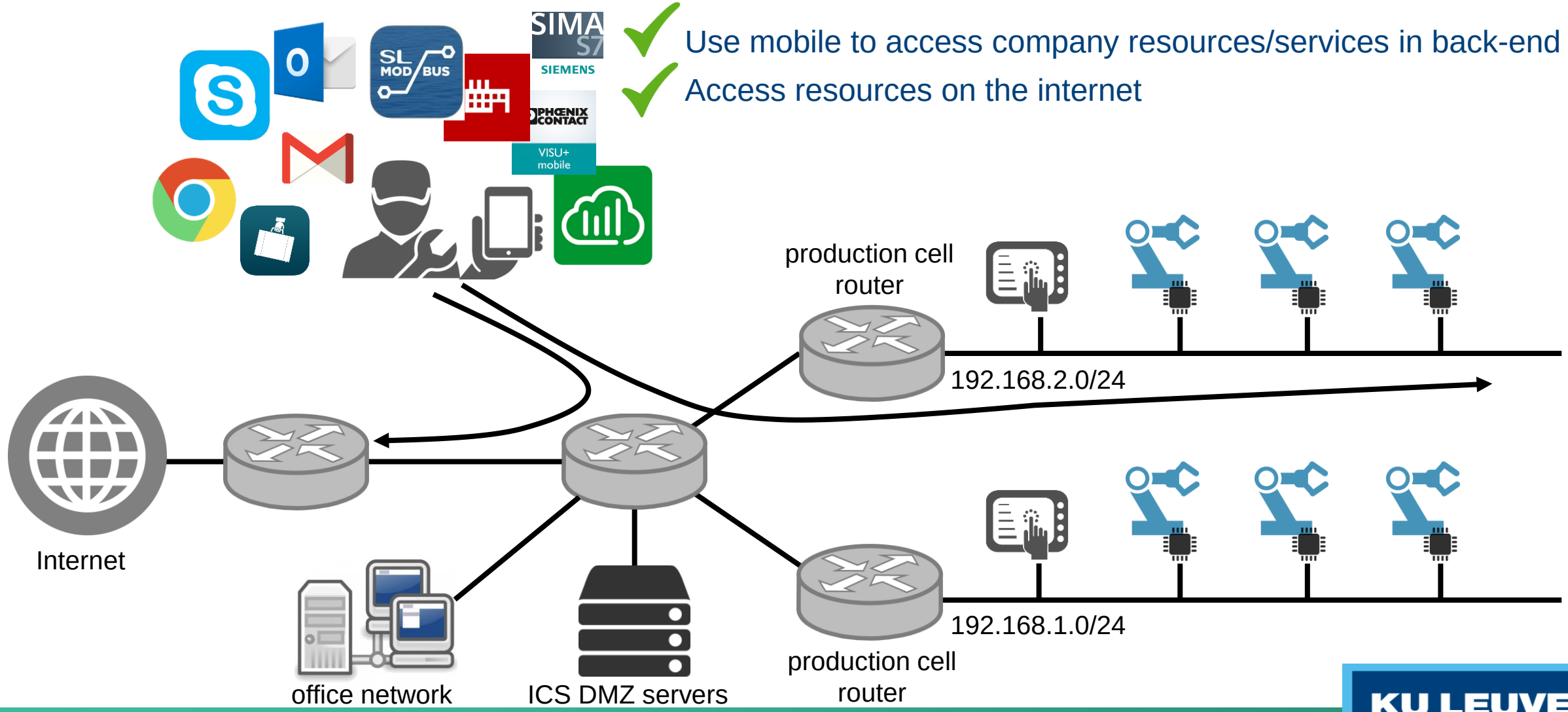
http://www.automationworld.com/mobility/industrial-mobile-apps-whos-using-them-and-why

https://library.e.abb.com/public/c6c714440006c741c1257ad200492e1b/46-51%204m213_EN_72dpi.pdf

KU LEUVEN

Goals

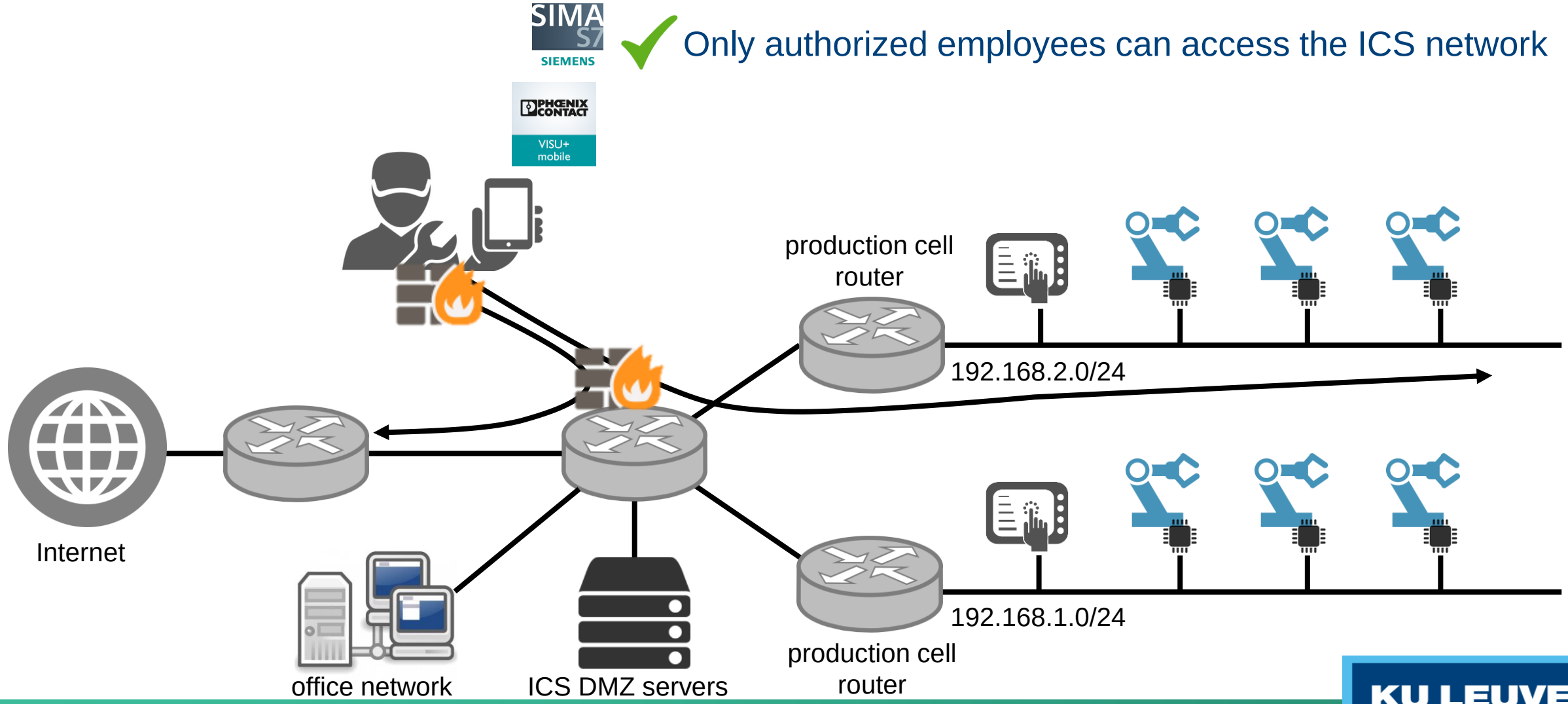
- ✓ Use mobile to interact with ICS equipment
- ✓ Use mobile to access company resources/services in back-end
- ✓ Access resources on the internet



KU LEUVEN

Goals

- ✓ Only traffic from specified ICS apps can reach the ICS network
- ✓ Only authorized employees can access the ICS network

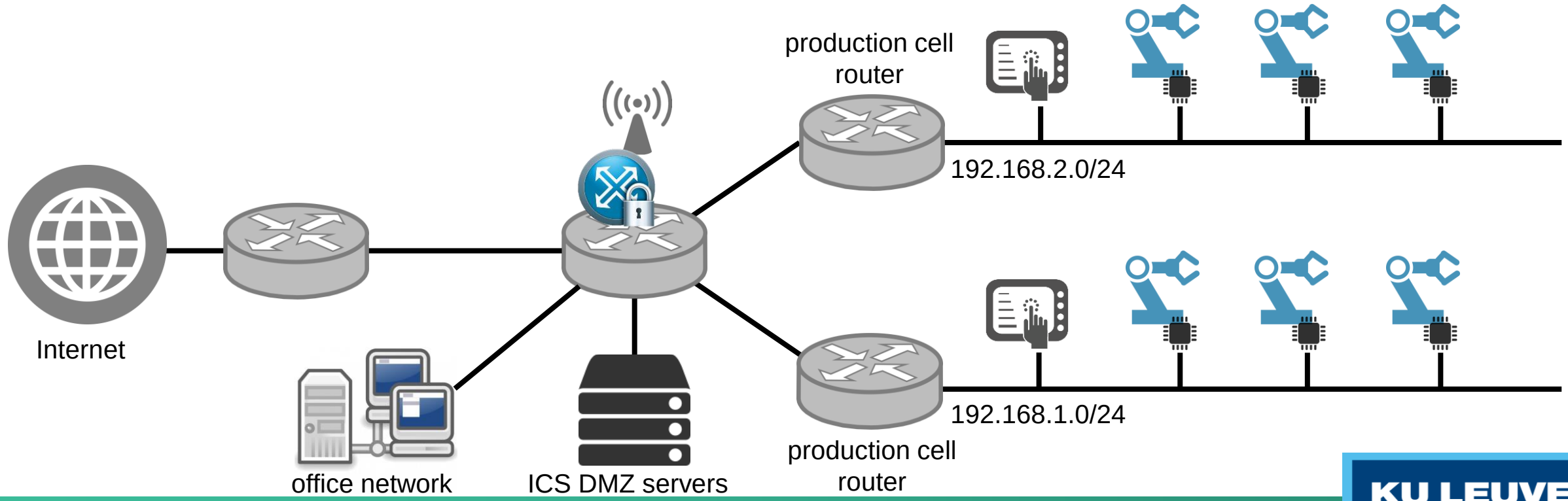


KU LEUVEN

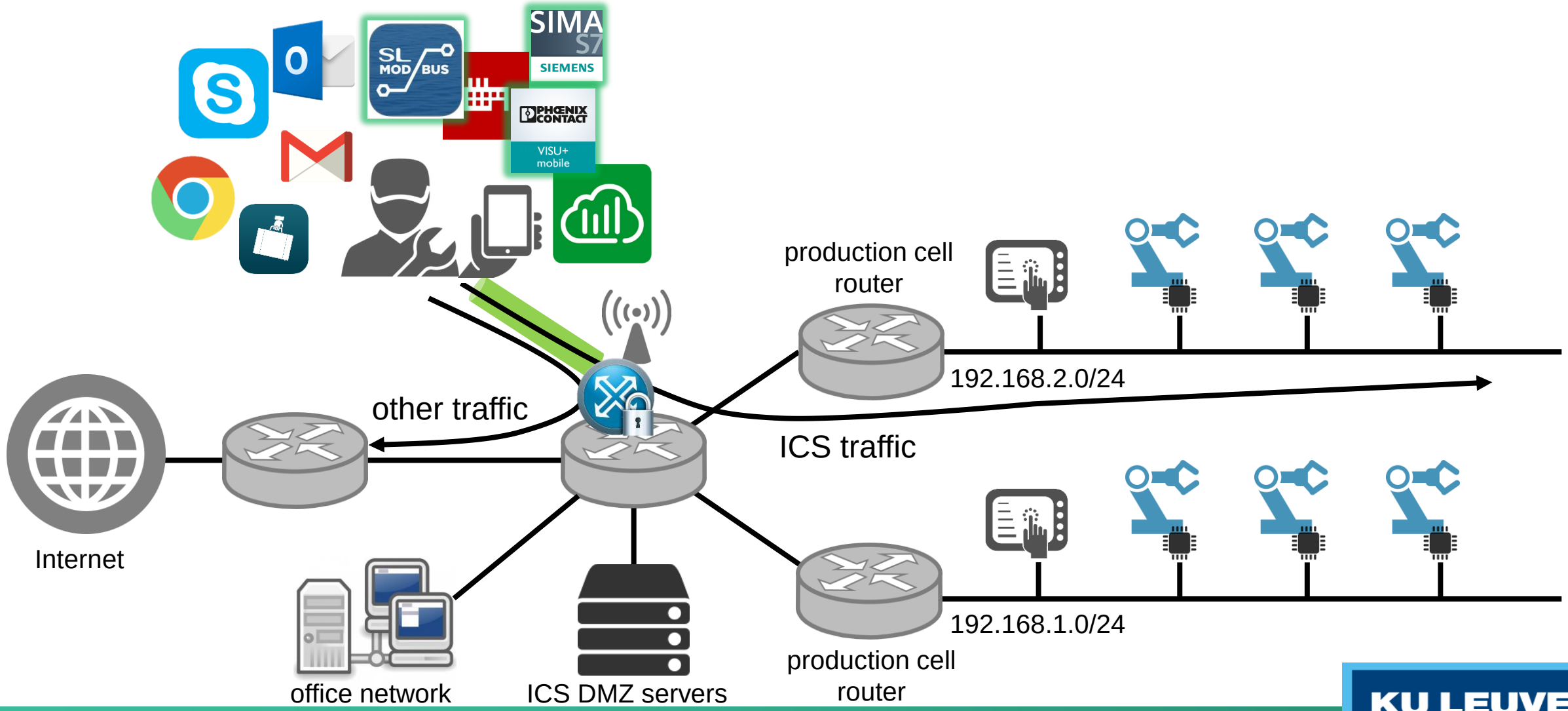
Setup

1. Wireless VPN gateway provides authenticated access to ICS network

2. MDM restricts apps that can access VPN interface on mobile device



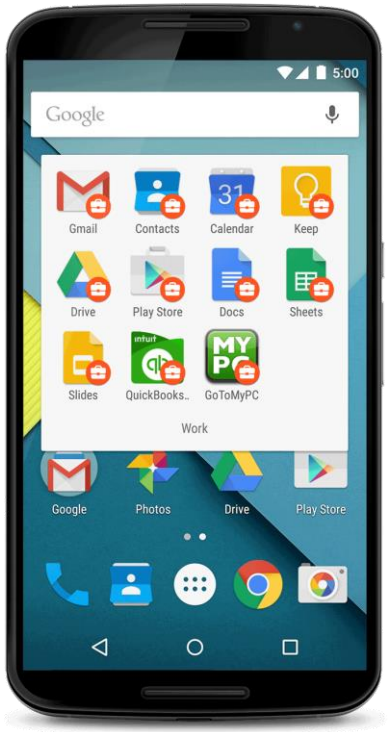
Setup



KU LEUVEN

Realisation

- Uses the Android for Work platform
  - Improve Android usability, security, and flexibility in work environments
  - Built-into recent Android devices (5 and higher)

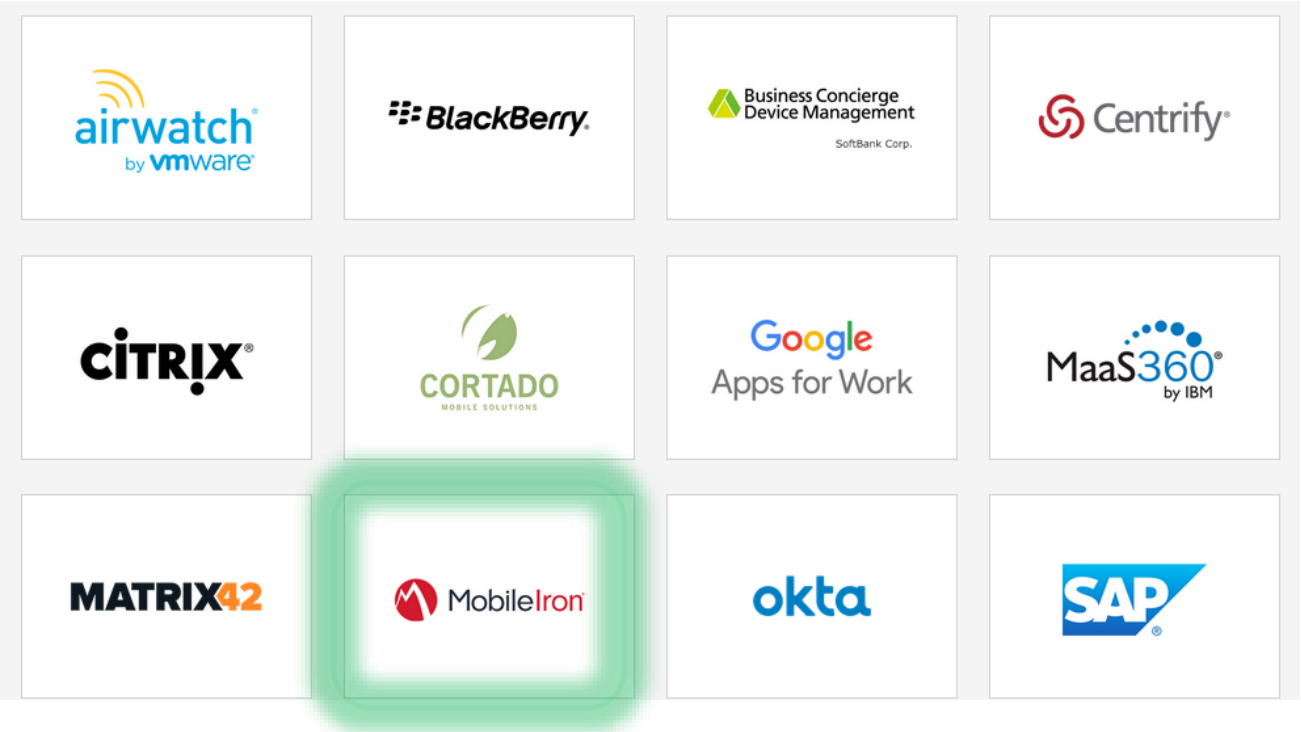


  - Supports two virtual profiles on Android device
    - Person profile managed by user
    - Work profile managed by employer
    - General security policies set by employer
  - User has both work and personal apps installed
    - Users can have the same app installed in both the work and personal profile
    - Sandboxing between both profiles

KU LEUVEN

Realisation

- Enterprise mobility management (EMM) providers provide the interface to manage devices using the AfW framework



Realisation

policies

MobileIron

policies

- VPN configuration
  - Crypto parameters
  - Endpoint address
  - CA certificate
  - Client certificate
  - Client key
- Selected ICS apps
- Platform security policies

Conclusion

- More in-depth analysis can be found on project website
  - https://msec.be/verboten/
- Fully supported by commercial MDM providers
- Similar possibilities for iOS
- Prototype demo during break

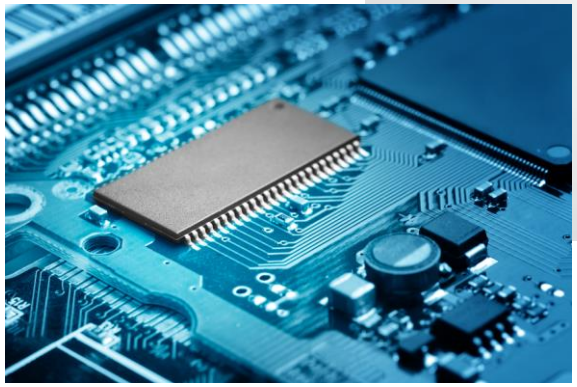
Secure Services on Embedded Android in Industrial Settings

KU LEUVEN

Introduction

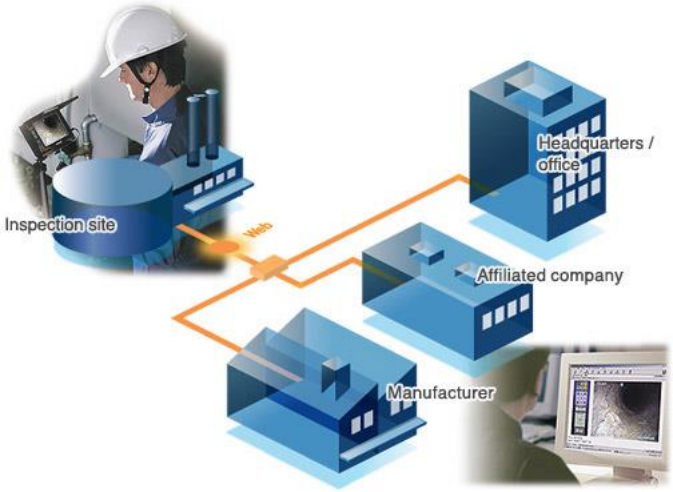
INTERNET OF THINGS

Plattform INDUSTRIE 4.0

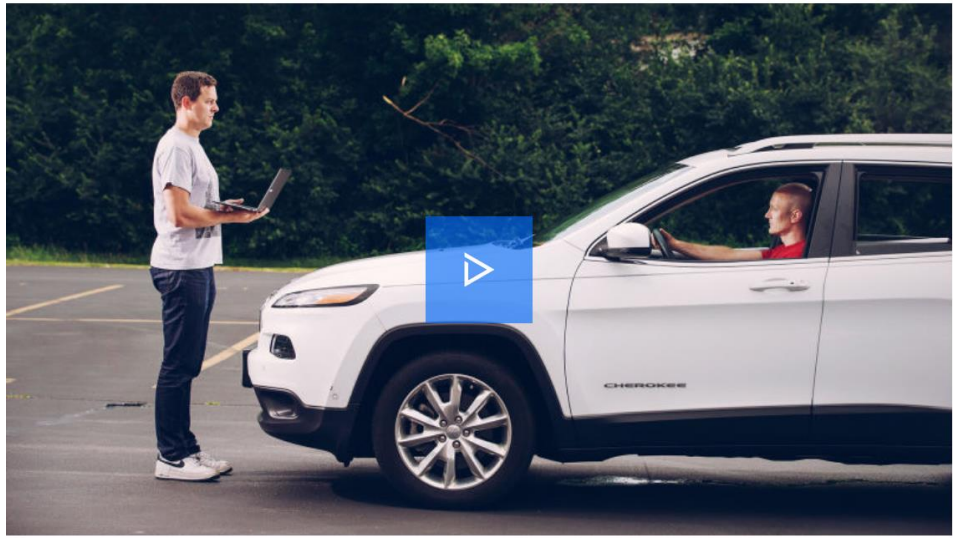


KU LEUVEN

Introduction



HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



KU LEUVEN

Our approach

KU LEUVEN

Secure Service Example

- Robot arm workspace secured with laser sensor

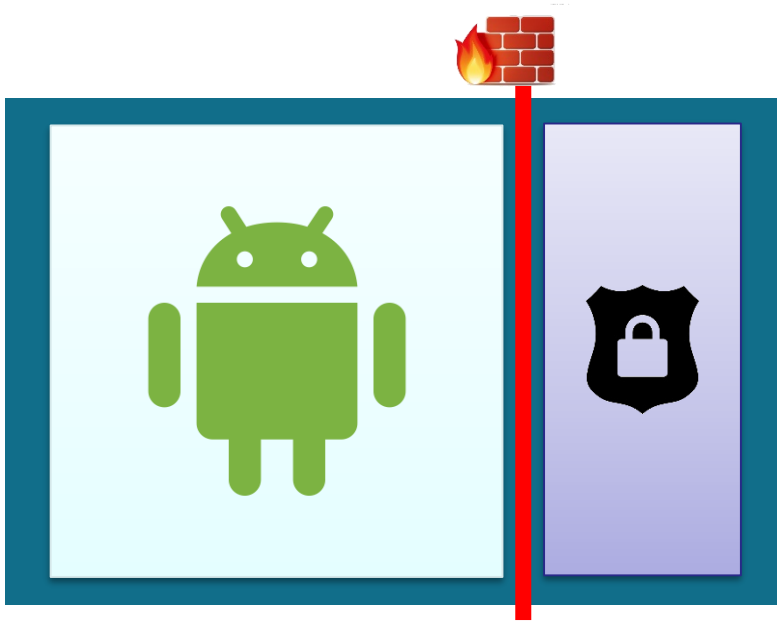
- Secure service: Disable robot arm as soon as laser is broken

How does it work?

- Isolate part of the platform from Android
- Isolated section has higher security guarantees
- Uses ARM TrustZone technology

TrustZone®
Security Foundation by ARM®

- Prototype developed on SabreLITE board

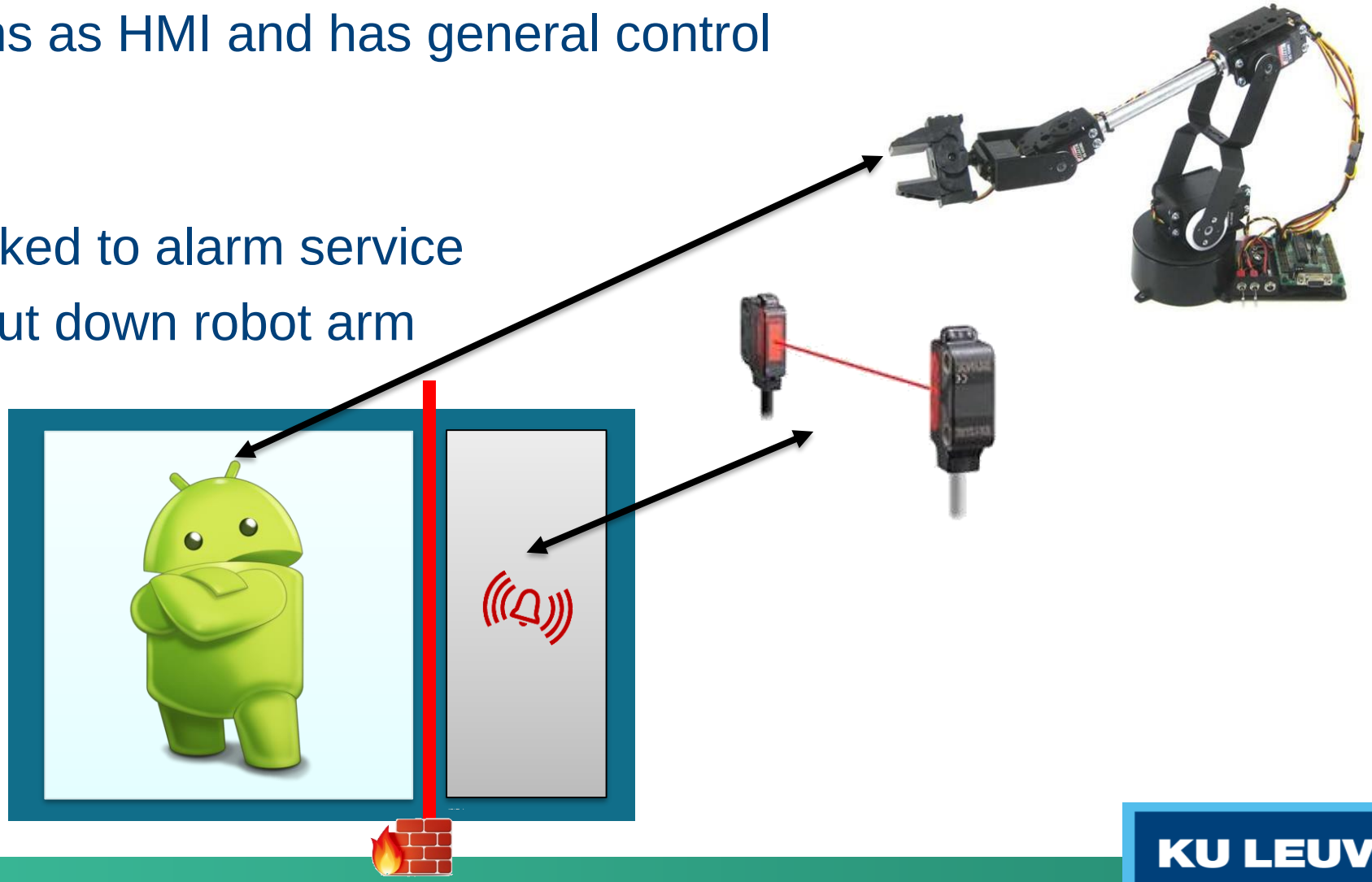


KU LEUVEN

Robot Arm

- Android functions as HMI and has general control over robot arm

- Laser sensor linked to alarm service
  - Alarm can shut down robot arm

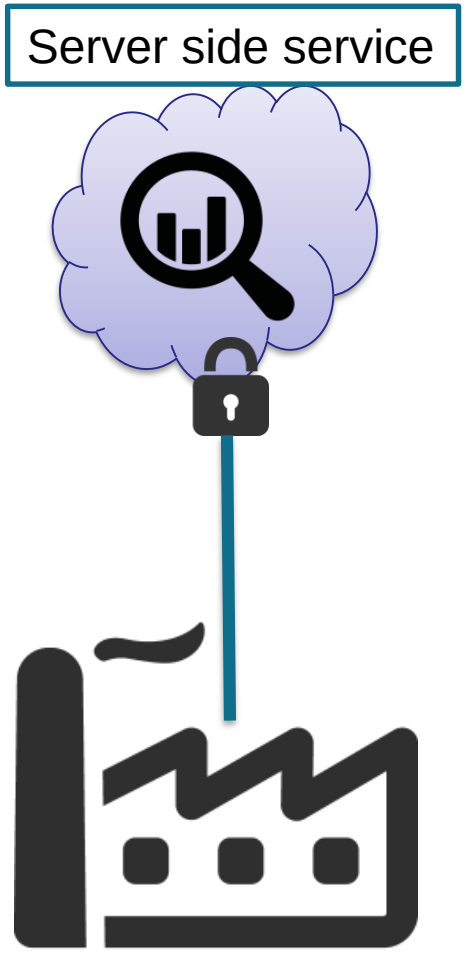


Proprietary Software

- Company specialised in production floor analysis
- Offers the analysis as service to its clients
- Production floor can be optimized based on the results

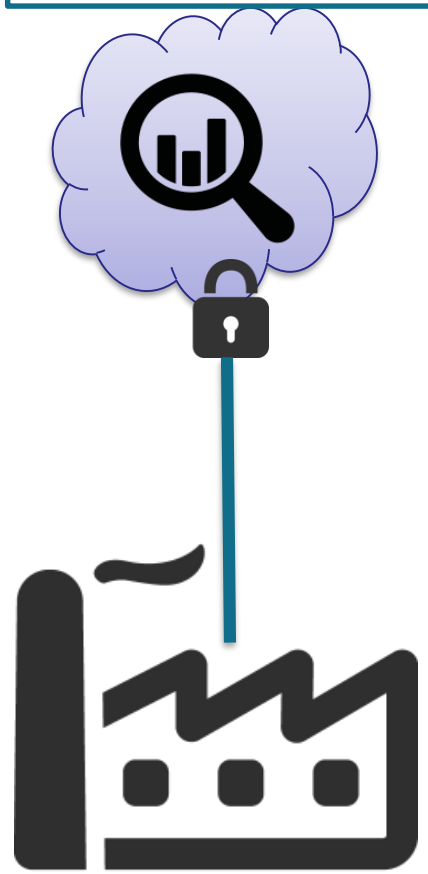
KU LEUVEN

Proprietary software

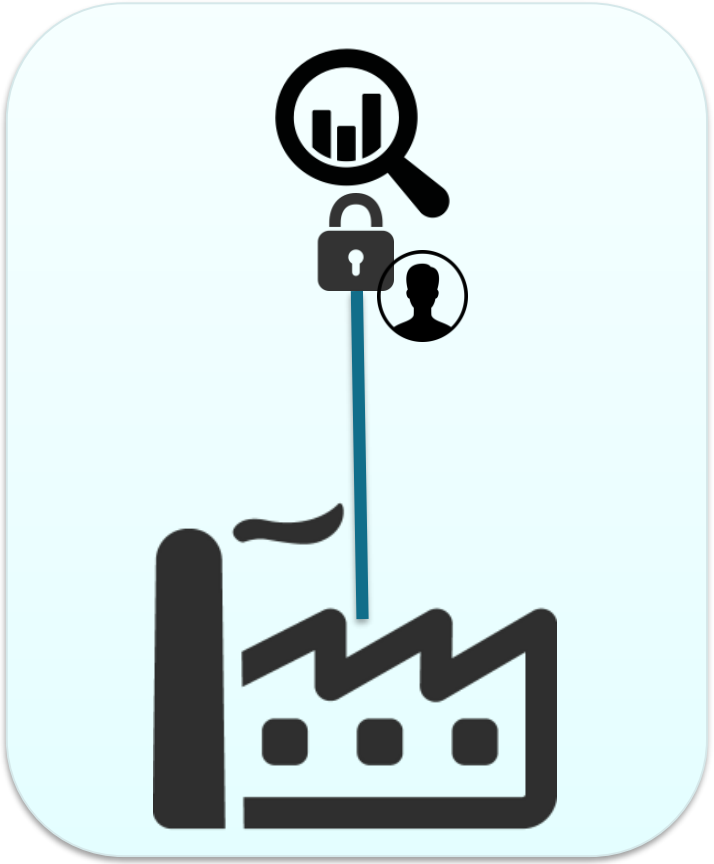


Proprietary software

Server side service



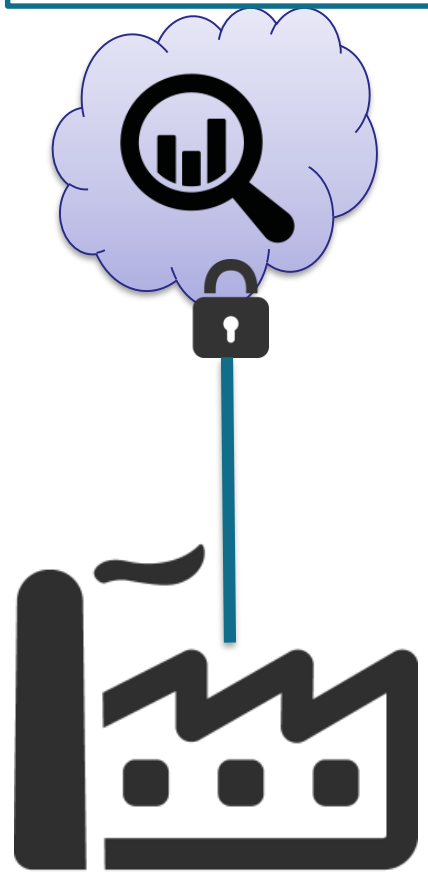
Dedicated device



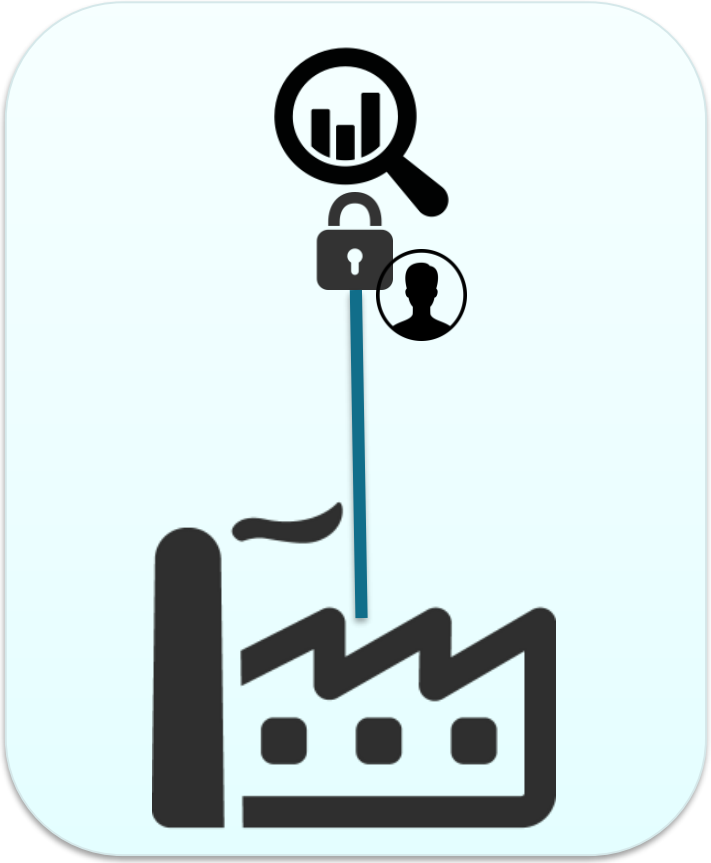
KU LEUVEN

Proprietary software

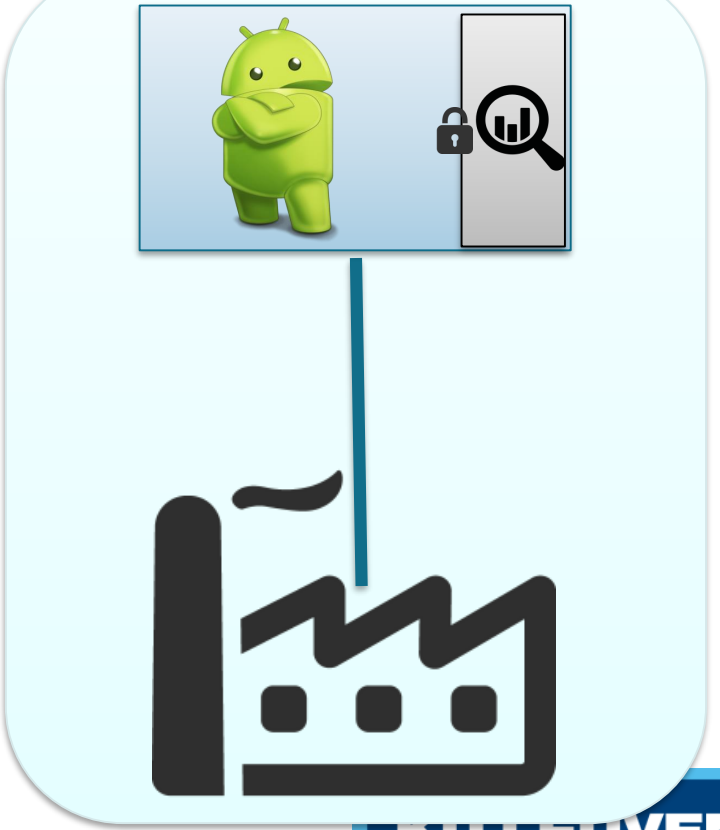
Server side service



Dedicated device



Our approach



Leasing Machines

- Company leases machines to clients
- Price based on usage
- Android used as HMI and control
- Isolated partition creates authenticated logs

Conclusion

- Android platform can be used to provide secure services
  - Data confidentiality and authenticity
  - Critical services can run unimpeded

- These services can enable new business cases or amplify existing work

KU LEUVEN