



# Agile and Secure Manufacturing on the Field Level

**Contact:**
**Hans-Peter Huth (Author)**
**Dr. Amine M. Houyou (Project Coordinator)**
**Siemens AG Corporate Technology,**
**hans-peter.huth(at)siemens.com, amine.houyou(at)siemens.com**
**http://www.iot-at-work.eu/**

# IoT@Work Project

## EU funded Project

- Duration: 3 years
- Approx. 3.5 Mio € Funding (Total Budget ~ 5.9 Mio € )
- Started on June 2010
- 6 Partners from Industry and Research

## Vision

- IoT Enabling Agile Manufacturing Systems

| | |
|---|---|
| SIEMENS | Project coordinator<br>network & security |
| Microsoft Innovation Center Europe | Security<br>Configuration Management |
| FIAT GROUP / CRF / CENTRO RICERCHE FIAT | Scenarios & requirements<br>pilot |
| TXT e-solutions | Software engineering &<br>middleware aspects |
| CITY UNIVERSITY LONDON | Software engineering<br>system modelling |
| inIT Institut Industrial IT www.init-owl.de | Automation & engineering |

## IoT - our definition

# Internet of Things

# =

# Connected Things & Services

## IoT@Work Hypothesis:

- A focus on interactions between embedded devices, machines, things
  - **Communication** between Things and Services (Network as a service)
  - One important application domain **"Factory Automation"**
- The IoT is an enabler to ***flexibility and agility*** of production systems

## General Goals for Automation Environments

- Reduce engineering costs
- Reduce maintenance costs and system downtime
- Increase flexibility and reduce re-configuration costs
- Reduce infrastructure costs

***IoT@Work = (Reliable communication) + (Secure Plug&Work) + (Web-technologies)***

## Approach

- **One network infrastructure** with standardized Internet protocols
- **Seamless inter communication** of domains and services, e. g. enterprise management, office network, remote maintenance, automation
- **Internet** technologies and **Web** technologies **down to the field**
- Ease the commissioning process with **auto-configuration** mechanisms

# Requirements

## Industrial Automation Requirements

- from extensive study of real world scenarios

## Functional

- decoupling of applications and underlying infrastructure
- decoupling of stakeholders
- security: device integrity, network access control, application capabilities

## Non-Functional

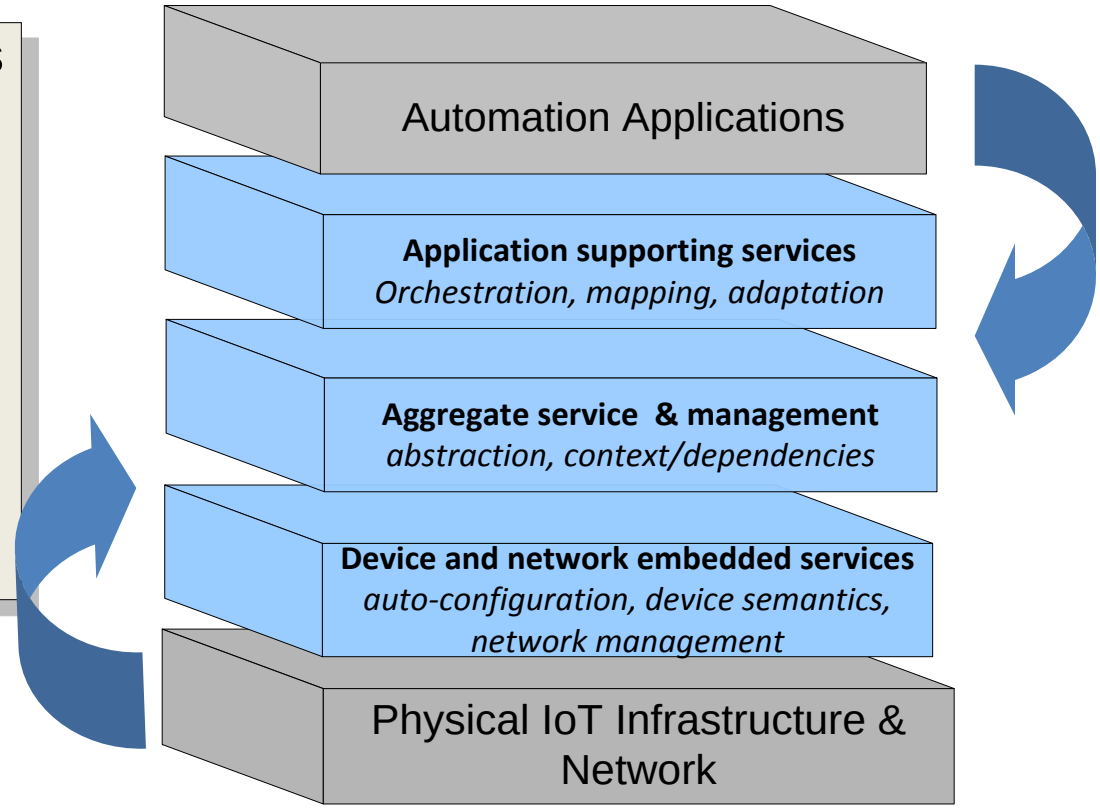
- industrial performance & reliability
- scalable to thousands of devices
- low configuration efforts
- dependable and predictable

# IoT@Work Architecture Approach

## Tomorrow

Loose coupling of applications to things

- Planning of applications and resources decoupled
- Auto configuration
- Far less efforts for configuration and commissioning
- Enhanced flexibility

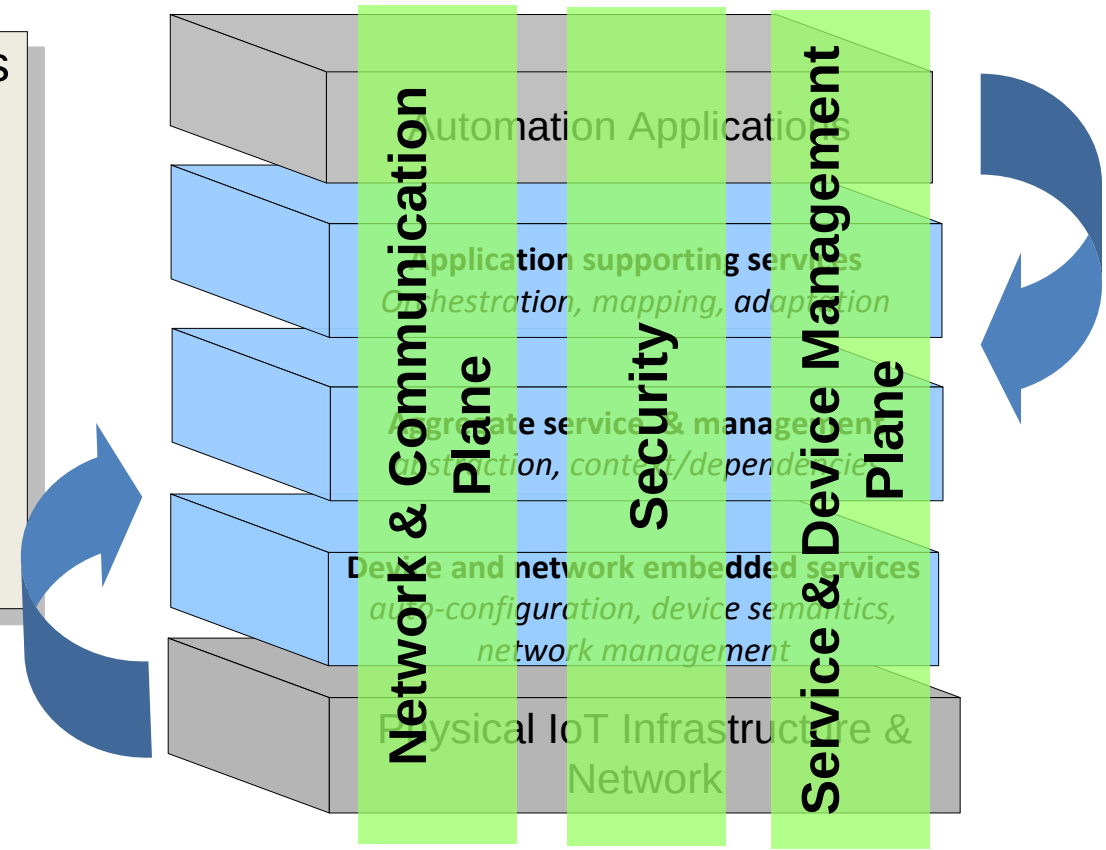


# IoT@Work Architecture Approach

## Tomorrow

- Planning of applications and resources decoupled
- Auto configuration
- Far less efforts for configuration and commissioning
- Enhanced flexibility

Planes to achieve inter-layer information flow

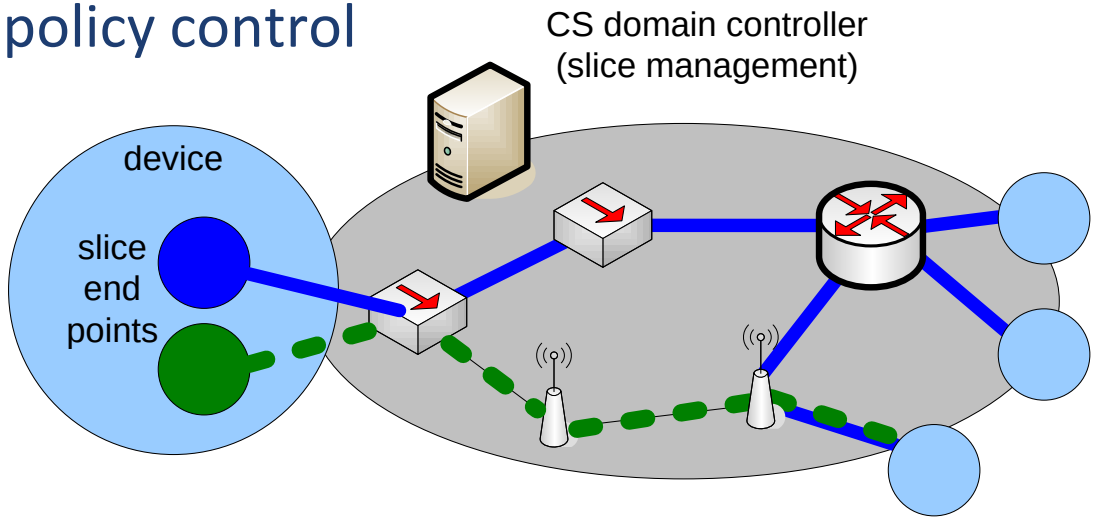


# Middleware Services

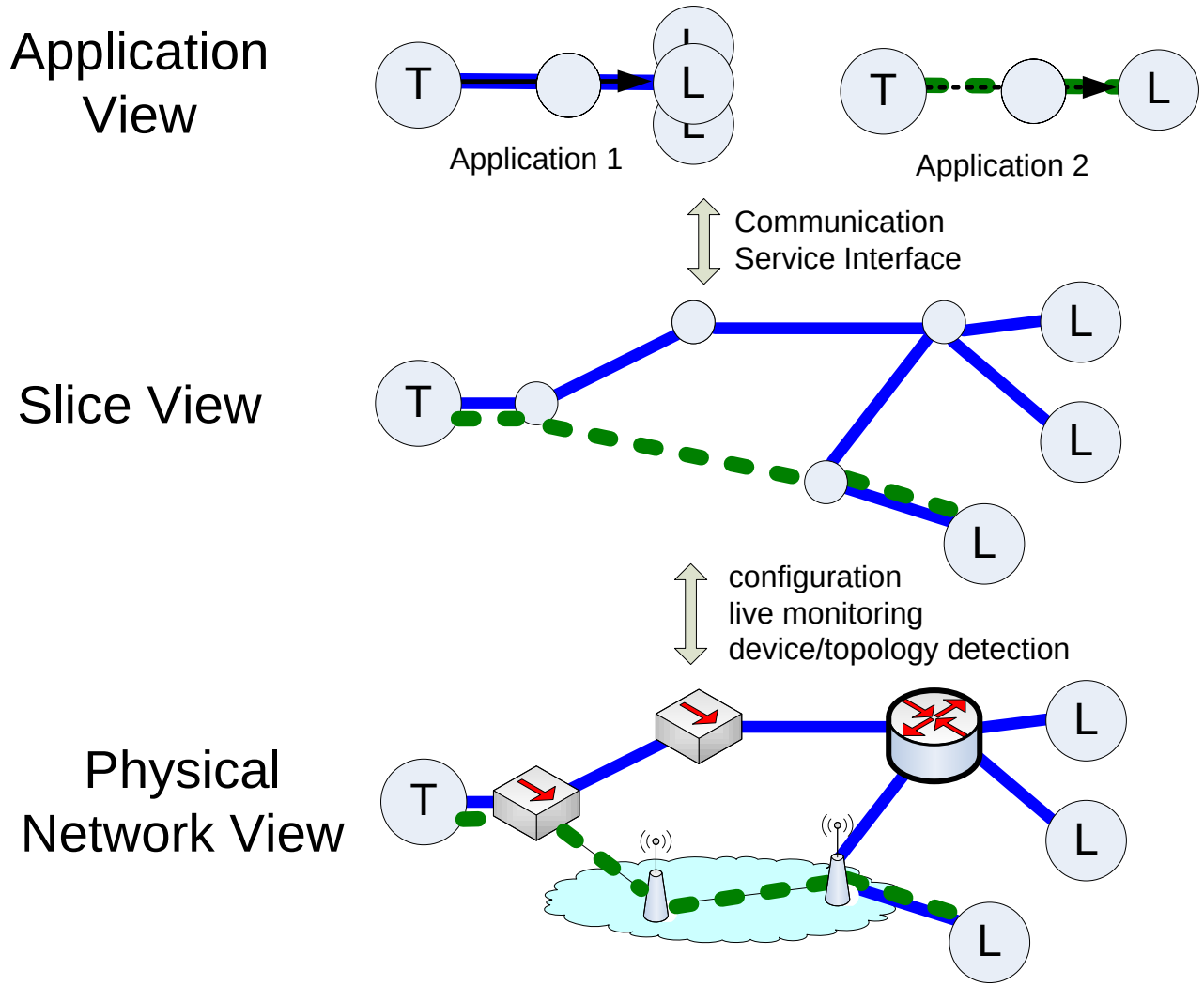
- **Abstractions** (e.g., semantics, localization).
- **Optimizations** (e.g., scalable messaging, caching) or other commonly used services (e.g., monitoring, eventing).
- **Security**
- Components include:
  - **Cross layer functions**: monitoring, discovery, logging, presence, ...
  - The **Event Notification Service** (ENS)
  - **Capability & Security Management**
  - **Directory Service**

# Network and Communication Services:

- **Localization** of devices in the network (topological)
- **Connectivity** services with support of:
  - reliability - i.e. fast failure recovery
  - scalability - support aggregates
  - network access control & policy control
  - QoS
- **Resource Management**
- **Network Virtualization**
- **Self-Configuration**



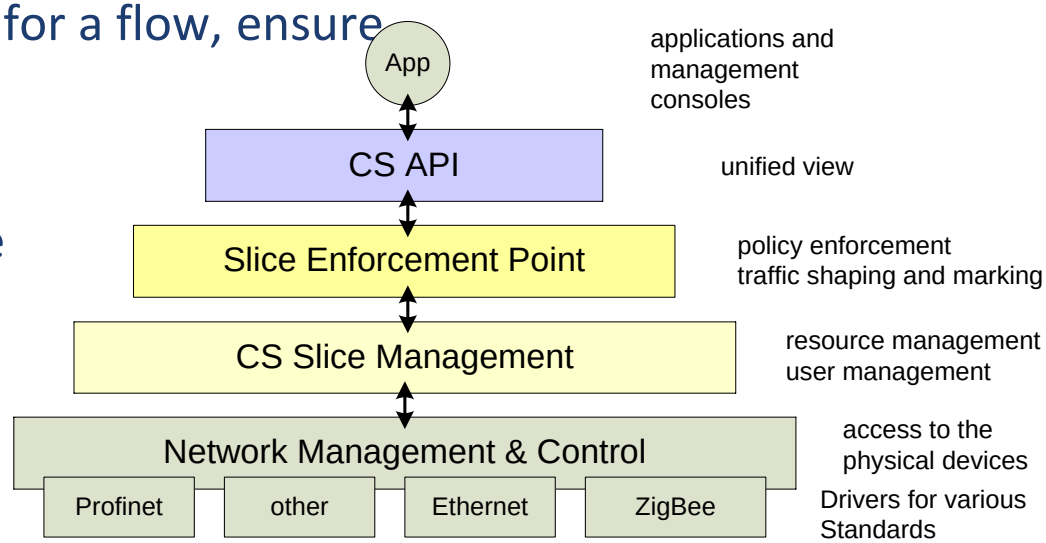
# Network Abstraction




- network abstraction for the applications
- slice = virtualisation + resource management + security
- field level allows re-use of Industrial Standards
- live -management done from the slice layer

# The IoT@Work Slice Concept

- **slice - a definition**
  - **virtualisation + resource management + security**
  - network protocol independent view
  - manages QoS, policy control and resilience
    - i.e. enforce maximum bandwidth for a flow, ensure minimum
  - mapping to field level technologies:
    - i.e. Profinet, AVB, VLAN and more
    - automatic commissioning,
      i.e. on-the-fly VLAN configuration
- **intelligent live management**
  - optimisations, failure handling
  - autonomous operation but based on rules from the planning phase



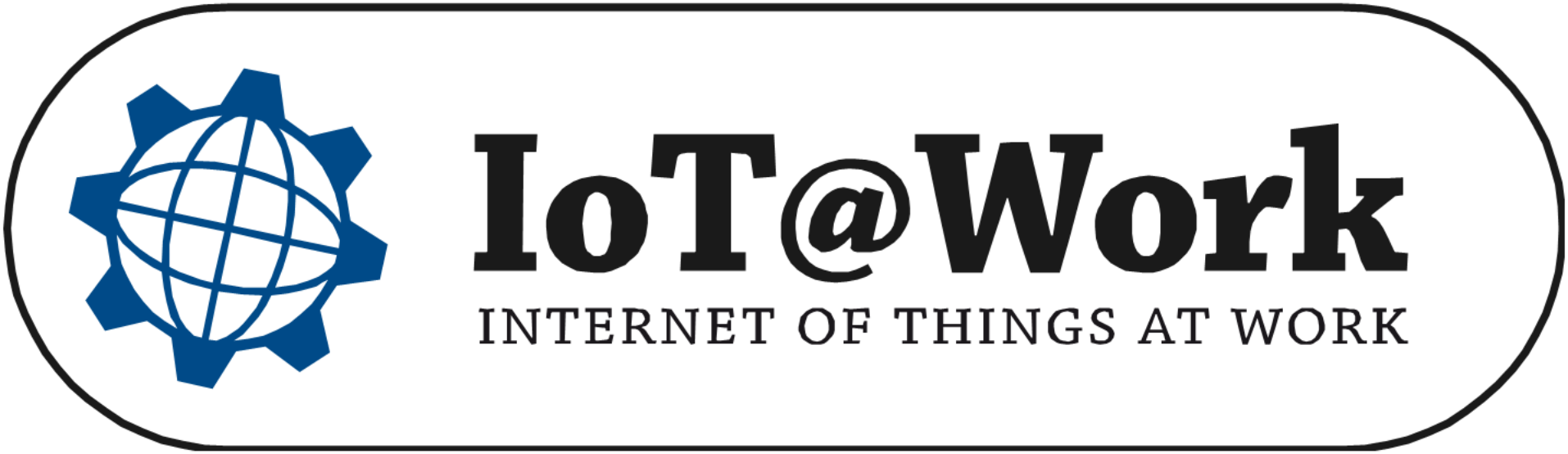
## Auto Configuration of Automation Devices

- **Service oriented architecture for industrial Ethernets using OPC-UA (inIT)**
  - provide auto-configuration for automation devices
  - re-use the well known OPC-UA standard
  - i.e. for initial device configuration after boot
  - proof-of-concept for Profinet IO
- **Slice Interface on Devices**
  - allows for different slices per application
  - slice auto-configuration controlled by boot-scripts and the slice manager

# Conclusion

- **IoT@Work applies and adopts IoT for Industrial Automation**
- **Evolve current Industrial Standards** towards more flexibility, auto-configuration and higher security
- **Cornerstones**:
  - **virtualisation integrating resource management and security**
  - **live network management**
  - **decoupling planning, commissioning and operation**
  - **auto-configuration on all levels while still staying predictable and planable**

# Conclusion




## Interesting?

more info:

**www.iot-at-work.eu**

**Thank You**

**Hans-Peter Huth, Siemens AG**