Future of Manufacturing – A View on Web of Things and Services

Guido Stephan, Head of Networks & Communication at the Research and Technology Center, Siemens Corporate Technology
The Future of Manufacturing –
A view on Web of Things and Services
Guido Stephan
From the Internet to a Web of Things

Internet

Research Networks

World Wide Web

Web2.0

Internet / Web of Things

ARPANET  TCP/IP  http  VoIP  Mobile Web  Social Media  M2M  Smart Grid  Smart City

Web of Things – two different views

Data Centric Approach
Cloud Services + Internet of Things = Big Data

Information Centric Approach
Smart Things + Internet = Web of Things

- Trust
- Proof
- Logic
- Rules / Query
- Ontology
- RDF Model & Syntax
- XML Query
- XML Schema
- XML
- Namespaces
- Unicode
- URI / IRI

Smart „Thing“

- Algorithms
- Data
- Ontology
- Web Service
What makes a thing and thing in WoT?

Things are aggregates which deliver information and services others need for their own functionality.

"Fractal" view on Things and Webs:
- Smart Grid
- Building
- HVAC
- Sensor

From a small sensor to a large building, depending on the viewpoint and task.

Composition of Things:
- Connectivity
  - Can be managed and integrated
- Intelligence
  - Can perform analytics and interact
- Flexibility
  - Can manage and run SW applications and services

From simple connectivity to full-blown smart things running SW applications.
The Future of Manufacturing:
Three key elements

1. Production network
   Flexible value chains with information available in real-time across company boundaries

2. Fusion of virtual and real world
   Integration of product design and production engineering for shorter time to market

3. Cyber-physical systems
   Modular production units with complete and consistent virtual image
Production based on cyber-physical systems

“Smart” products
- The product to be manufactured has all the necessary information for every step of its production

Modular production units
- Optimized organization of networked production facilities taking into account the entire value chain
- Production steps are configured flexibly in response to changing situations

Reduction of complexity due to “smarter” structures
Cyber-physical systems have all the information as a digital model

Cyber-physical system (CPS)

Physical production facility + Digital model

Contains all the information on:
- Software / Informatics
- Mechanics
- Electrics, Electronics
- Automation, HMI
- Safety, security
- Maintenance
- Location, identity...
- Status
- SW version
- Interfaces
- ...

The digital model is always up-to-date and is extended over the entire lifecycle

Product design → Production planning → Production engineering → Production execution → Services
Example for discrete industries:
Covering entire product and production lifecycles

Product design | Production planning | Production engineering | Production execution | Services

---

PLM Software  | PLM TIA | Totally Integrated Automation
What needs to be done!

**Today**
- Local controls
- Realtime communication
- Digital "copies" of products and production
- Manufacturing Execution Systems
- Industrial security concepts
- Execution and decision making mainly by humans

**Future**
- Dynamic network of local controls
- Extended complex communication
- Digital models of the overall process and participants
- Process optimization in dynamic networks
- Self-configuring security concepts also for temporary requirements
- Humans to define rules and frameworks for decision making

- Rule framework and architecture for dynamic topologies
- Massively extended semantics for M2M communication
- Integrated process simulation
- ...
Research Challenge 1:
Safety and Security in an open and interconnected industrial WoT

Paradigm shift towards open, interconnected IT systems → rising complexity

Overall goals:
- improving usability,
- reducing complexity and
- optimizing the cost structure of secure products & solutions

<table>
<thead>
<tr>
<th>Security questions</th>
<th>Requirements of an industrial environment</th>
<th>Security Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication of a device</td>
<td>Lean management of identities, access rights and keys for industrial devices and users</td>
<td>Managed Identities &amp; Access</td>
</tr>
<tr>
<td>What is it?</td>
<td></td>
<td>- Public Key Infrastructure (PKI)</td>
</tr>
<tr>
<td>Authorization of a device</td>
<td>Trust within the device: unforgettable identity, protection of credentials, authenticated access to data and commands</td>
<td>- Identity and Access Management (IAM)</td>
</tr>
<tr>
<td>What is the device allowed to do?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust in device</td>
<td>Confidential, authenticated and integrity-checked information flow, reliable and in time</td>
<td>Trust Anchor within the device</td>
</tr>
<tr>
<td>Interaction between systems</td>
<td></td>
<td>- Modular Crypto Library</td>
</tr>
<tr>
<td>How do devices communicate in a secure, reliable way</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Unrestricted © Siemens AG 2014. All rights reserved
Different factors are driving the demand for industrial security

**New Functionality**
- Example:
  - Device connectivity

**Security Use Case**
- Examples:
  - Know-how protection
  - I 4.0 scenarios

**Quality of Security**
- Examples:
  - Attack robustness
  - Long term security
Research Challenge 2
Semantic Technologies as Enabler for flexible self organizing production

Autonomous production modules dynamically collaborate through semantic services

Pre-configuration

Electrical Engineering
Mechanical Engineering

Dynamic orchestration

Model-driven design

Software Engineering

Semantic Technologies

...to semantic services

Production Ontology

Autonomous Cyber Physical Modules

...via functional descriptions...

From bits and bytes...

Instruction List

Sequential Function Chart

Source: Adapted from Prof. Zühike, DFKI
How to deal with the installed base?

We need to ensure backwards compatibility as well as interoperability!
Research Challenge 3
WoT Standardization

Application diversity

- Internet of Things (IoT) will be an enabler for various new applications in many application areas ranging from industrial to home and personal areas
- Diverse applications have a diverse set of requirements for considering for example availability, reliability, security, safety, latency, delay, bandwidth, footprint and costs

Technology diversity

- IoT covers a broad set of technology areas starting from lower layer communication technologies to semantics and knowledge representation.
- Various solutions already exist for these technologies areas and many new solutions will be introduced

Standardization diversity

- Many IoT specific or related standardization activities have been initiated by standardization development organizations, consortia and fora worldwide
- Many standards already exist for the application areas and have to be taken into account in order to have a smooth transition to IoT

➤ How to achieve interoperability with such a diversity of applications, technologies and standards?
## WoT Standardization

No “One Fits All” – Approach for WoT Architecture reasonable

<table>
<thead>
<tr>
<th>Strive for interoperability where it is needed</th>
<th>A framework to derive “interworkable” domain specific IoT architectures</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Full interoperability between each and every IoT device and application is not needed. The closer things and applications act together, the higher level of interoperability is needed</td>
<td>• Various application domains will have their specific architectures based on use cases, requirements and specific deployment scenarios</td>
</tr>
<tr>
<td>• Use gateways to bridge between different domains and technologies</td>
<td>• An IoT Architecture Framework allows to build IoT architectures with large (underlying) similarity in as many use-case domains as feasible</td>
</tr>
<tr>
<td>• Use semantic web technologies to ensure that data can be comprehended unambiguously across different platforms and domains</td>
<td></td>
</tr>
</tbody>
</table>

➤ **Have a common model, view and language, similar to the OSI 7 layer model, to achieve the required levels of interoperability**
WoT Standardization
The WoT Architecture Framework

WoT Architectural Framework

IoT Architectural Reference Model
- Reference model
- Reference architecture
- Guidance
- Common language
- Common architectural elements
- Multiple use-case domains
- Common domain view and entities
- Controls architecture divergence

Domain & Application specific

Application-specific IoT Architecture (e.g., Distribution Automation)

Transformation

Domain-specific IoT Model (Profile)

Profiling & Guidance

Smart Grids

Digital Factory

Smart Buildings

Intelligent Transport Domain & Application specific

Application-specific IoT Architecture (e.g., Smart Metering)

Profiling & Guidance

Transformation

Unrestricted © Siemens AG 2014. All rights reserved
Web of Things: Web-based integration and interaction of smart distributed systems

Massive Distributed Systems: Plug and automate for massively distributed systems

Embedded Networks: Standard IT technologies for networked embedded systems

Industrial Communication: Reliable communication with guaranteed quality for industrial applications
Thank you!
Many thanks for your attention!

Guido Stephan  
Head of Technology Field  
Siemens AG / Germany / CT RTC NEC  
Otto-Hahn-Ring 6  
81739 Munich  
Phone: +49 (89) 636-52950  
Fax: +49 (89) 636-51115  
Mobile: +49 (173) 7074426  
E-mail: stephan.guido@siemens.com  
siemens.com/innovation
Please complete the brief breakout session survey that can be found in the mobile app under "Surveys."

Your input is essential in helping the IoTWF steering committee improve the quality of sessions for IoTWF 2015.

If you haven’t already downloaded the app, you can do so at customers.genie-connect.com/iotwf2014 on your mobile device.