Welcome!

Thank you for joining us on a panel session on: Monitoring and Evaluating the Cyber-Health of Industrial Control Systems
## Table of Contents

**Moderated Session on Monitoring and Evaluating the Cyber-Health of Industrial Control Systems**

**13:45 to 13:55**
1) Welcome!
2) Table of Contents
3) Session Information
4) Introduction of Panelists

**13:55 to 14:15**
5) What are Industrial Control Systems (ICS)?
6) What Constitutes Cyber Health for ICS?
7) What Aspects of Cyber are the Panelists Covering?
8) Review of Topics Covered

**14:15 to 14:55**
9) Remarks from Panelists

**14:55 to 15:30**
10) Let the Debate Begin!
11) Questions and Answers
# Table of Contents

**Moderated Session on Monitoring and Evaluating the Cyber-Health of Industrial Control Systems**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:45 to 13:55</td>
<td>1) Welcome!</td>
</tr>
<tr>
<td></td>
<td>2) Table of Contents</td>
</tr>
<tr>
<td></td>
<td>3) Session Information</td>
</tr>
<tr>
<td></td>
<td>4) Introduction of Panelists</td>
</tr>
<tr>
<td>13:55 to 14:15</td>
<td>5) What are Industrial Control Systems (ICS)?</td>
</tr>
<tr>
<td></td>
<td>6) What Constitutes Cyber Health for ICS?</td>
</tr>
<tr>
<td></td>
<td>7) What Aspects of Cyber are the Panelists Covering?</td>
</tr>
<tr>
<td></td>
<td>8) Review of Topics Covered</td>
</tr>
<tr>
<td>14:15 to 14:55</td>
<td>9) Remarks from Panelists</td>
</tr>
<tr>
<td>14:55 to 15:30</td>
<td>10) Let the Debate Begin!</td>
</tr>
<tr>
<td></td>
<td>11) Questions and Answers</td>
</tr>
</tbody>
</table>
Session 13:45 to 15:30

Moderator:
Dr. Steve Chan, Massachusetts Institute of Technology (MIT), USA

Panelists:
♦ Dr. Rainer Falk, Siemens AG, Corporate Technology, Deutschland
♦ Dr. Maria Bada, Global Cyber Security Capacity Centre, University of Oxford, United Kingdom
♦ Dr. Xing Liu, Kwantlen Polytechnic University, Canada
♦ Dr. Daniel Kästner, AbsInt Angewandte Informatik GmbH, Germany
## Table of Contents

### Moderated Session on Monitoring and Evaluating the Cyber-Health of Industrial Control Systems

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Activities</th>
</tr>
</thead>
</table>
| 13:45 to 13:55 | 1) Welcome!  
                  2) Table of Contents  
                  3) Session Information  
                  4) Introduction of Panelists                                  |
| 13:55 to 14:15 | 5) What are Industrial Control Systems (ICS)?  
                  6) What Constitutes Cyber Health for ICS?  
                  7) What Aspects of Cyber are the Panelists Covering?  
                  8) Review of Topics Covered                                     |
| 14:15 to 14:55 | 9) Remarks from Panelists                                              |
| 14:55 to 15:30 | 10) Let the Debate Begin!                                               |
|            | 11) Questions and Answers                                               |
Introduction of Panelist Members

Panelist:
Dr. Rainer Falk,
Siemens AG, Corporate Technology,
Deutschland

Focus:
Industrial Cyber Security:
◊ Application of industrial security standard IEC 62443;
◊ Security in industrial IoT / Industry 4.0.
Introduction of Panelist Members

Panelist:
Dr. Maria Bada,
Global Cyber Security Capacity Centre, University of Oxford,
United Kingdom

Focus:
Impact of cyber attacks on users and society as a whole (social, psychological, cultural, economic, political, etc.):
◊ How lack of training or awareness can lead to people not following procedures or requirements, thus leading to potential risks;
◊ Multi-layer impact of attacks.
Introduction of Panelist Members

Panelist:
Dr. Xing Liu,
Kwantlen Polytechnic University,
Canada

Focus:
Embedded Systems for Cyber-Physical Systems:
◊ Embedded Microprocessors;
◊ Embedded Operating Systems.
Introduction of Panelist Members

Panelist:
Dr.-Ing. Daniel Kästner,
AbsInt Angewandte Informatik GmbH,
Germany

Focus:
Current and future security challenges in safety-critical systems:
◊ Suitable methods to demonstrate safety and security properties.
# Table of Contents

## Moderated Session on Monitoring and Evaluating the Cyber-Health of Industrial Control Systems

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Details</th>
</tr>
</thead>
</table>
| 13:45 to 13:55 | 1) Welcome!  
2) Table of Contents  
3) Session Information  
4) Introduction of Panelists |
| 13:55 to 14:15 | 5) What are Industrial Control Systems (ICS)?  
6) What Constitutes Cyber Health for ICS?  
7) What Aspects of Cyber are the Panelists Covering?  
8) Review of Topics Covered |
| 14:15 to 14:55 | 9) Remarks from Panelists  
10) Let the Debate Begin!  
11) Questions and Answers |

14:55 to 15:30

Tuesday 11/14/17 13:45-15:30
What are Industrial Control Systems (ICS)?

Panelists:
- Dr. Rainer Falk, Siemens AG, Corporate Technology, Deutschland
- Dr. Maria Bada, Global Cyber Security Capacity Centre, University of Oxford, United Kingdom
- Dr. Xing Liu, Kwantlen Polytechnic University, Canada
- Dr. Daniel Kästner, AbsInt Angewandte Informatik GmbH, Germany
Table of Contents

Moderated Session on Monitoring and Evaluating the Cyber-Health of Industrial Control Systems

13:45 to 13:55
1) Welcome!
2) Table of Contents
3) Session Information
4) Introduction of Panelists

13:55 to 14:15
5) What are Industrial Control Systems (ICS)?
✓ 6) What Constitutes Cyber Health for ICS?
7) What Aspects of Cyber are the Panelists Covering?
8) Review of Topics Covered

14:15 to 14:55
9) Remarks from Panelists

14:55 to 15:30
10) Let the Debate Begin!
11) Questions and Answers
What Constitutes Cyber Health for ICS?

Panelists:
◊ Dr. Rainer Falk, Siemens AG, Corporate Technology, Deutschland
◊ Dr. Maria Bada, Global Cyber Security Capacity Centre, University of Oxford, United Kingdom
◊ Dr. Xing Liu, Kwantlen Polytechnic University, Canada
◊ Dr. Daniel Kästner, AbsInt Angewandte Informatik GmbH, Germany
Table of Contents

Moderated Session on Monitoring and Evaluating the Cyber-Health of Industrial Control Systems

13:45 to 13:55
1) Welcome!
2) Table of Contents
3) Session Information
4) Introduction of Panelists

13:55 to 14:15
5) What are Industrial Control Systems (ICS)?
6) What Constitutes Cyber Health for ICS?
7) What Aspects of Cyber are the Panelists Covering?
8) Review of Topics Covered

14:15 to 14:55
9) Remarks from Panelists

14:55 to 15:30
10) Let the Debate Begin!
11) Questions and Answers
What Aspects of Cyber are the Panelists Covering?

- Cyberspace Operations
- Electromagnetic Spectrum Operations
- Electronic Warfare
- Cyberspace Electromagnetic Activities
Multiple Cyber Vulnerabilities...

At the Generation

At the Transmission

At the Distribution
# Table of Contents

**Moderated Session on Monitoring and Evaluating the Cyber-Health of Industrial Control Systems**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:45 to 13:55</td>
<td>1) Welcome! 2) Table of Contents 3) Session Information 4) Introduction of Panelists</td>
</tr>
<tr>
<td>14:15 to 14:55</td>
<td>9) Remarks from Panelists 10) Let the Debate Begin!</td>
</tr>
<tr>
<td>14:55 to 15:30</td>
<td>8) Review of Topics Covered</td>
</tr>
</tbody>
</table>

**Tuesday 11/14/17 13:45-15:30**

IARIA PANEL ON CYBER SYSTEMS: CYBER-CENTERED MAJOR CHALLENGES
Review of Topics Covered

◊ Protecting Industry 4.0 assets
◊ Industrial control systems monitoring and protection
◊ Cyber security for strategic/critical infrastructure, Germany
  ◊ Production-oriented big data protection
  ◊ Industrial IoT (Internet of Things) challenges
◊ Cyber-attacks on industrial communication protocols
◊ Device-oriented cyber monitoring
Table of Contents

Moderated Session on Monitoring and Evaluating the Cyber-Health of Industrial Control Systems

13:45 to 13:55
1) Welcome!
2) Table of Contents
3) Session Information
4) Introduction of Panelists

13:55 to 14:15
5) What are Industrial Control Systems (ICS)?
6) What Constitutes Cyber Health for ICS?
7) What Aspects of Cyber are the Panelists Covering?
8) Review of Topics Covered

14:15 to 14:55
✓ 9) Remarks from Panelists

14:55 to 15:30
10) Let the Debate Begin!
11) Questions and Answers
Remarks from Panelists
(in order as listed...)

Panelists:
◊ Dr. Rainer Falk, Siemens AG, Corporate Technology, Deutschland
◊ Dr. Maria Bada, Global Cyber Security Capacity Centre, University of Oxford, United Kingdom
◊ Dr. Xing Liu, Kwantlen Polytechnic University, Canada
◊ Dr. Daniel Kästner, AbsInt Angewandte Informatik GmbH, Germany
Remarks from Panelists

Panelists:

Dr. Rainer Falk, Siemens AG, Corporate Technology, Deutschland
Dr. Maria Bada, Global Cyber Security Capacity Centre, University of Oxford, United Kingdom
Dr. Xing Liu, Kwantlen Polytechnic University, Canada
Dr. Daniel Kästner, AbsInt Angewandte Informatik GmbH, Germany
Remarks from Panelists

Panelists:
- Dr. Rainer Falk, Siemens AG, Corporate Technology, Deutschland
- Dr. Maria Bada, Global Cyber Security Capacity Centre, University of Oxford, United Kingdom
- Dr. Xing Liu, Kwantlen Polytechnic University, Canada
- Dr. Daniel Kästner, AbsInt Angewandte Informatik GmbH, Germany
Remarks from Panelists

Panelists:

♢ Dr. Rainer Falk, Siemens AG, Corporate Technology, Deutschland
♢ Dr. Maria Bada, Global Cyber Security Capacity Centre, University of Oxford, United Kingdom
♢ Dr. Xing Liu, Kwantlen Polytechnic University, Canada
♢ Dr. Daniel Kästner, AbsInt Angewandte Informatik GmbH, Germany
Remarks from Panelists

Panelists:

♢ Dr. Rainer Falk, Siemens AG, Corporate Technology, Deutschland
♢ Dr. Maria Bada, Global Cyber Security Capacity Centre, University of Oxford, United Kingdom
♢ Dr. Xing Liu, Kwantlen Polytechnic University, Canada
♢ Dr. Daniel Kästner, AbsInt Angewandte Informatik GmbH, Germany
### Table of Contents

**Moderated Session on Monitoring and Evaluating the Cyber-Health of Industrial Control Systems**

**13:45 to 13:55**
1) Welcome!
2) Table of Contents
3) Session Information
4) Introduction of Panelists

**13:55 to 14:15**
5) What are Industrial Control Systems (ICS)?
6) What Constitutes Cyber Health for ICS?
7) What Aspects of Cyber are the Panelists Covering?
8) Review of Topics Covered

**14:15 to 14:55**
9) Remarks from Panelists

**14:55 to 15:30**
10) Let the Debate Begin!
11) Questions and Answers
# Table of Contents

**Moderated Session on Monitoring and Evaluating the Cyber-Health of Industrial Control Systems**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:45 to 13:55</td>
<td>1) Welcome!</td>
</tr>
<tr>
<td></td>
<td>2) Table of Contents</td>
</tr>
<tr>
<td></td>
<td>3) Session Information</td>
</tr>
<tr>
<td></td>
<td>4) Introduction of Panelists</td>
</tr>
<tr>
<td>13:55 to 14:15</td>
<td>5) What are Industrial Control Systems (ICS)?</td>
</tr>
<tr>
<td></td>
<td>6) What Constitutes Cyber Health for ICS?</td>
</tr>
<tr>
<td></td>
<td>7) What Aspects of Cyber are the Panelists Covering?</td>
</tr>
<tr>
<td></td>
<td>8) Review of Topics Covered</td>
</tr>
<tr>
<td>14:15 to 14:55</td>
<td>9) Remarks from Panelists</td>
</tr>
<tr>
<td>14:55 to 15:30</td>
<td>10) Let the Debate Begin!</td>
</tr>
<tr>
<td></td>
<td>✔️ 11) Questions and Answers</td>
</tr>
</tbody>
</table>
Thank You!

...for attending this IARIA Session: Monitoring and Evaluating the Cyber-Health of Industrial Control Systems
Safety and Security at the Code Level

Daniel Kästner
AbsInt GmbH, 2017
Common Sources of C Security Vulnerabilities

1. Stack-based buffer overflow
2. Heap-based buffer overflow
3. Further invalid pointer accesses (null, dangling, ...)
4. Uninitialized memory accesses
5. Integer errors
6. Format string vulnerabilities
7. Concurrency defects

! Safety-relevant defects
! Absence of such defects can be proven in safety-critical software, e.g., by sound static analysis.
Abstract Interpretation

- **Semantics** based methodology for program analysis
- Formal method – supports **correctness proofs**
  - **Efficiency**: scales to real-life industry applications due to abstractions
  - **Soundness**:
    - Correctness of abstractions **proven**.
    - **Never fail to report a defect** from the class of defects under analysis
  - **Safety**: over-approximate the program semantics. Some precision may be lost, but **always on the safe side**.
Proving the Absence of Runtime Errors

- Sound static analysis based on Abstract Interpretation.
- Astrée detects all runtime errors with few false alarms, incl:
  - Array index out of bounds
  - Int/float division by 0
  - Invalid pointer dereferences
  - Uninitialized variables
  - Arithmetic overflows
  - Data races
  - Lock/unlock problems, deadlocks
  - Floating point overflows and invalid operations (Inf and NaN)
  + Floating-point rounding errors taken into account
  + User-defined assertions, unreachable code, non-terminating loops
  + Check coding guidelines (MISRA C, CERT, CWE, ISO/IEC TS 17961)
  + Program slicer
Safety vs. Security

- **Functional Safety**
  - Absence of unreasonable risk to life and property caused by malfunctioning behavior of the system

- **Security**
  - Absence of harm caused by malicious (mis-)usage of the system

- **Observation**
  - Vulnerabilities often based on defects that might cause system to malfunction by itself
(Information-/Cyber-) Security Aspects

- **Confidentiality**
  - Information shall not be disclosed to unauthorized entities
  - safety-relevant

- **Integrity**
  - Data shall not be modified in an unauthorized or undetected way
  - safety-relevant

- **Availability**
  - Data is accessible and usable upon demand
  - safety-relevant

- **Safety**

  In some cases: not safe $\Rightarrow$ not secure
  In some cases: not secure $\Rightarrow$ not safe
Questions

1. Stronger security claims possible in safety-critical systems?
   - Proving absence of vulnerabilities?

2. Which attacks still feasible when C code is free of critical undefined/ unspecified behaviors?
   - Side channel attacks
   - Information disclosure via undesired program paths
   - ...?
Questions

3. Stronger requirements needed in case of safety-critical security-critical systems?

ISO-26262 Ed.2 DIS 2017
email: info@absint.com
http://www.absint.com
The Human Factor in Cyber Security

Dr Maria Bada
Global Cyber Security Capacity Centre
University of Oxford
Maria.Bada@cs.ox.ac.uk
@MariaBadaOxford
The Human Factor in Cyber Security

Factors in Security Breaches

- 52% Human error
- 48% Technology error

Top Human Error Sources

- 42% End user failure to follow policies and procedures
- 42% General carelessness
- 31% Failure to get up to speed on new threats
- 29% Lack of expertise with websites/applications
- 26% IT staff failure to follow policies and procedures

Trends in Information Security Copyright (c) 2015 CompTIA Properties, LLC. All Rights Reserved. | CompTIA.org
The Security, Functionality and Usability Triangle
The Human Factor in Cyber Security
Insider Threats - Accidental

**Incident:** Government Breach
A State health-assistance program informed 14,000 individuals that it had accidentally published their Social Security numbers.

**Breach:** Accidentally published sensitive information that remained up on a government site for at least nine days before it was removed.

**Impact:** Similar breaches in the past exposed the personally identifiable information of more than 750,000 persons in multiple incidents within the same State.

(The CERT® Insider Threat Team, August 2013)
The Human Factor in Cyber Security
Insider Threats – Malicious Intent

Edward Snowden: He released sensitive NSA documents, before fleeing the country, that became a blow-up about government surveillance.

Army Private First Class Bradley Manning (Chelsea): He released sensitive military documents to WikiLeaks. He was given a sentence of 35 years in prison.
The Human Factor in Cyber Security
Lack of Awareness
Subjects and Impact of Cyber Attacks

- Physical
- Psychological / emotional
- Political / governmental
- Reputational
- Cultural
- Economic
THANK YOU!

Dr Maria Bada
Global Cyber Security Capacity Centre,
University of Oxford
maria.bada@cs.ox.ac.uk
@MariaBadaOxford
Panel on CYBER SYSTEMS: Enhancing Integrity Protection for Industrial Cyber Physical Systems

Dr. Rainer Falk
Office world versus industrial systems - Protection targets for security

**Industrial Systems:**
Protection of Production Resources

- Lifetime up to 20 years and more

**Office IT:**
Protection of IT-Infrastructure

- Lifetime 3-5 years
The CIA pyramid is turned upside down in industrial automation and control systems: “Protect Productivity”
Industrial systems and office world have different management & operational characteristics

<table>
<thead>
<tr>
<th>Protection target for security</th>
<th>Production resources, incl. logistics</th>
<th>Office IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component Lifetime</td>
<td>Up to 20 years</td>
<td>IT- Infrastructure</td>
</tr>
<tr>
<td>Availability requirement</td>
<td>Very high</td>
<td>3-5 years</td>
</tr>
<tr>
<td>Real time requirement</td>
<td>Can be critical</td>
<td>Medium, delays accepted</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Very much varying</td>
<td>Delays accepted</td>
</tr>
<tr>
<td>Application of patches</td>
<td>Slow / restricted by regulation</td>
<td>High (for IT Service Centers)</td>
</tr>
<tr>
<td>Anti-virus</td>
<td>Uncommon, hard to deploy, white listing</td>
<td>Regular / scheduled</td>
</tr>
<tr>
<td>Security testing / audit</td>
<td>Increasing</td>
<td>Common / widely used</td>
</tr>
</tbody>
</table>

Office IT:
- IT- Infrastructure
- 3-5 years
- Medium, delays accepted
- Delays accepted
- High (for IT Service Centers)
- Regular / scheduled
- Common / widely used
- Scheduled and mandated
Security-by-Design is different from Safety-by-Design

**Cyber Security**
Prevention of consequences of threats to a system (intentionally) caused by humans and/or environment

**Safety**
Prevention of threats to humans and environment caused by technical systems
Caught between regulation, requirements, and standards

Solution design and deployment plays an essential role in designing compliant solutions

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
<th>Compliance Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Owner</td>
<td>Operates and maintains</td>
<td>• ISO 27001/19&lt;br&gt;• IEC 62443-2-1&lt;br&gt;• NERC-CIP</td>
</tr>
<tr>
<td>System Integrator</td>
<td>Designs and deploys</td>
<td>• IEC 62443-2-4&lt;br&gt;• IEC 62443-3-3&lt;br&gt;• DIN VDE V0831-104&lt;br&gt;• BDEW WP</td>
</tr>
<tr>
<td>Product Supplier</td>
<td>Develops and supports</td>
<td>• IEC 62443-3-3&lt;br&gt;• IEC 62443-4-1&lt;br&gt;• IEC 62443-4-2&lt;br&gt;• BDEW WP</td>
</tr>
<tr>
<td></td>
<td>Design + hand over / maintain a secure solution</td>
<td>• ISO 27001/19&lt;br&gt;• IEC 62443-2-1&lt;br&gt;• NERC-CIP&lt;br&gt;• IEC 62443-2-4&lt;br&gt;• IEC 62443-3-3&lt;br&gt;• DIN VDE V0831-104&lt;br&gt;• BDEW WP</td>
</tr>
<tr>
<td></td>
<td>Secure operation, policies, requirements</td>
<td>• ISO 27001/19&lt;br&gt;• IEC 62443-2-1&lt;br&gt;• NERC-CIP&lt;br&gt;• IEC 62443-2-4&lt;br&gt;• IEC 62443-3-3&lt;br&gt;• DIN VDE V0831-104&lt;br&gt;• BDEW WP</td>
</tr>
<tr>
<td></td>
<td>Capabilities, documentation, secure development, support</td>
<td>• ISO 27001/19&lt;br&gt;• IEC 62443-2-1&lt;br&gt;• NERC-CIP&lt;br&gt;• IEC 62443-2-4&lt;br&gt;• IEC 62443-3-3&lt;br&gt;• DIN VDE V0831-104&lt;br&gt;• BDEW WP</td>
</tr>
</tbody>
</table>
### IEC 62443 Covers Security Management, System, and Component Level for Industrial Automation Control Systems (IACS)

#### General
- 1-1 Terminology, concepts and models
- 1-2 Master glossary of terms and abbreviations
- 1-3 System security compliance metrics
- 1-5 IACS Protection Levels

#### Definitions
- Metrics

#### Policies and procedures
- 2-1 Establishing an IACS security program
- 2-2 Operating an IACS security program
- 2-3 Patch management in the IACS environment
- 2-4 Certification of IACS supplier security policies

#### Requirements to the security organization and processes of the plant owner and suppliers

#### System
- 3-1 Security technologies for IACS
- 3-2 Security assurance levels for zones and conduits
- 3-3 System security requirements and security assurance levels

#### Requirements to a secure system

#### Component
- 4-1 Product development requirements
- 4-2 Technical security requirements for IACS products

#### Requirements to secure system components

IEC 62443 (ISA-99)
Security within Industry 4.0:
Security by design & security by default

More integrated security within applications
- …rather than just within the network (layers)
- Application based end-to-end security must be possible

Adaptive security architectures
- Agile security profiles have to be adaptable in a dynamic way.
- Fast configuration must include security.

Security for the digital model
- Security for the physical instance, its digital twin and their interactions must take place in a concerted way.

Prevention and reaction are still needed
- Security will remain moving target. There will be no final I4.0 security solution without a need for further measures.
Security has to be suitable for the addressed environment

Awareness and Acceptance

Since security is not just a technical solution, which can be incorporated transparently, we need to consider how humans can get along with this issue. This needs, especially for automation environments, actions for:

• awareness trainings
• help people to understand security measures and processes
• provide user friendly interfaces and processes
Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens’ products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

Siemens’ products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer’s exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/industrialsecurity.
Dr. Rainer Falk
Principal Key Expert
Siemens AG
Corporate Technology
CT RDA ITS
Otto-Hahn-Ring 6
D-81739 Munich
Germany
E-mail
rainer.falk@siemens.com
Internet
siemens.com/corporate-technology
Embedded Systems for Internet of Things (IoT)
- A Brief Overview

Xing Liu
Kwantlen Polytechnic University
CANADA
Observations

• The IoT *things* are supposed to be smart
• Smart *things* demand more computing power
• Novel **embedded systems** are being developed to meet the challenges
• These embedded systems include **processors** and corresponding **software**
Processors

• They are similar to traditional microcontrollers (CPU, memory, input/output); plus new functions
• They are named IoT processors
• The new functions include
  ▪ Wireless connectivity (Wi-Fi, Bluetooth Low Energy, …)
  ▪ Security (starting with electronic design)
  ▪ Power management and energy harvesting
Software

• Operating systems are now preferred for IoT devices
• They are named IoT OSes
• They are similar to operating systems in PC but smaller
  ▪ Multitasking, memory management, file structure, device I/O
• They also have functions including
  ▪ Supporting connectivity (software stack for Wi-Fi, Bluetooth Low Energy, …)
  ▪ Supporting security (managing security zones for device ID/keys, …)
  ▪ Supporting power management (wake up timing, …)
  ▪ Sensor drivers
Emerging IoT Processors

• SoC (system on chip) electronic chips (millimeter scale)

• Examples:
  - ARM Cortex-M23 and ARM Cortex-M33
  - Texas Instruments: CC3220
  - Qualcomm: Snapdragon 410 processor
  - Broadcom: BCM4343W SoC Module
  - Cypress: PSoC 6
Emerging IoT Boards

• Credit-card size or smaller boards
• Examples:
  ▪ mangOH Red board (Sierra Wireless)
  ▪ Raspberry Pi board (Raspberry Pi Foundation)
Emerging IoT OSes

• Software running on proprietary IoT processors or popular microcontrollers
  ▪ mbed OS (ARM)
  ▪ Contiki OS (contiki-os.org)
  ▪ Android Things (was Google Brillo; Google)
  ▪ RIOT OS (riot-os.org)
  ▪ Windows 10 IoT Core (Microsoft)
Summary

• Novel embedded systems (IoT processors, IoT boards and IoT OSes) are on the rise
• They provide the foundations for IoT applications such as smart homes and smart cities