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

Table of Contents

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

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

Introduction of Panelist Members

<u>Panelist</u>:
Dr. Rainer Falk,
Siemens AG, Corporate Technology,
Deutschland

<u>Focus</u>:
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

<u>Panelist</u>:
Dr. Xing Liu,
Kwantlen Polytechnic University,
Canada

<u>Focus</u>:
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

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

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

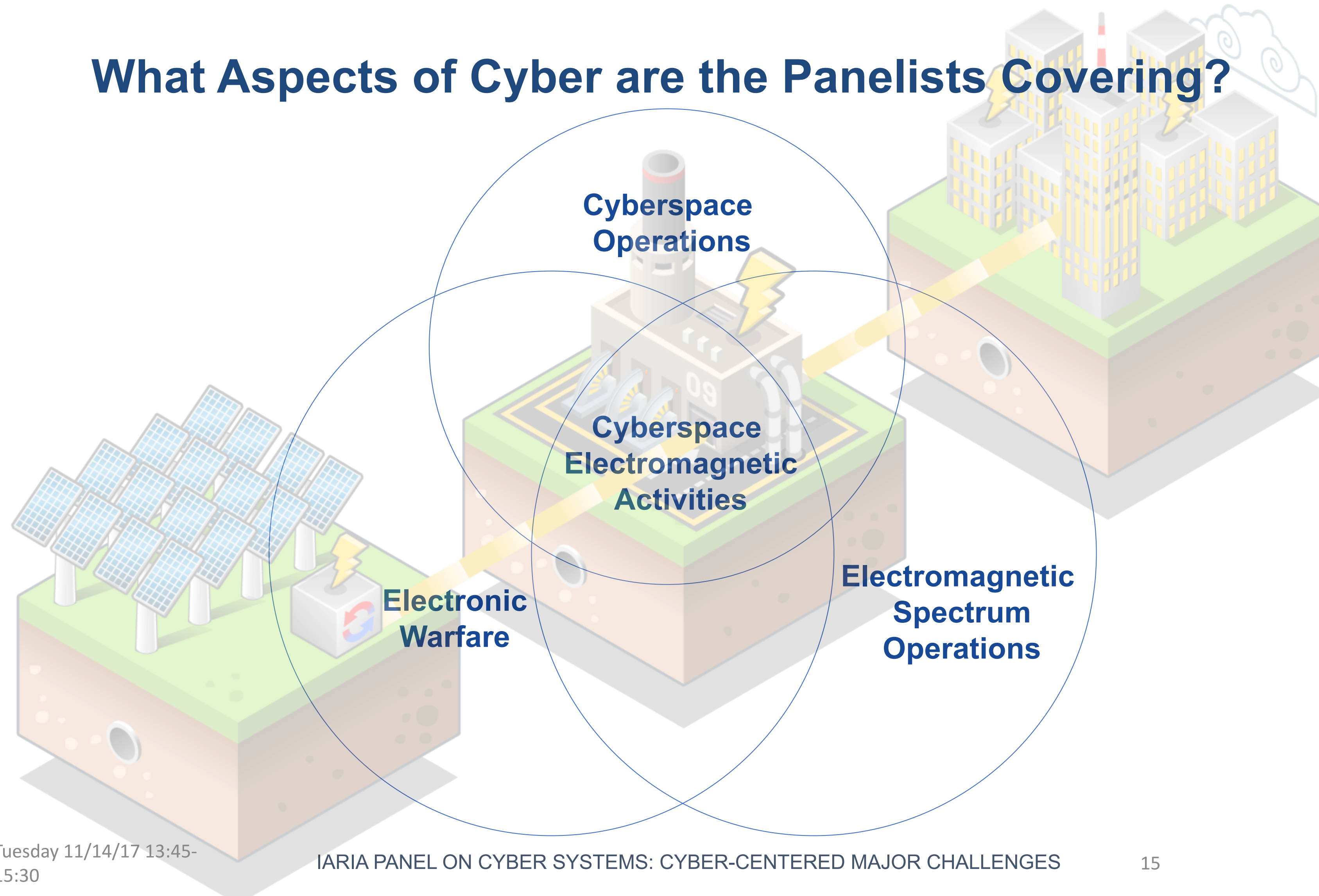
◊ Dr. Xing Liu, Kwantlen Polytechnic University, Canada

◊ Dr. Daniel Kästner, AbsInt Angewandte Informatik GmbH, Germany

Table of Contents

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

What Aspects of Cyber are the Panelists Covering?



Multiple Cyber Vulnerabilities…

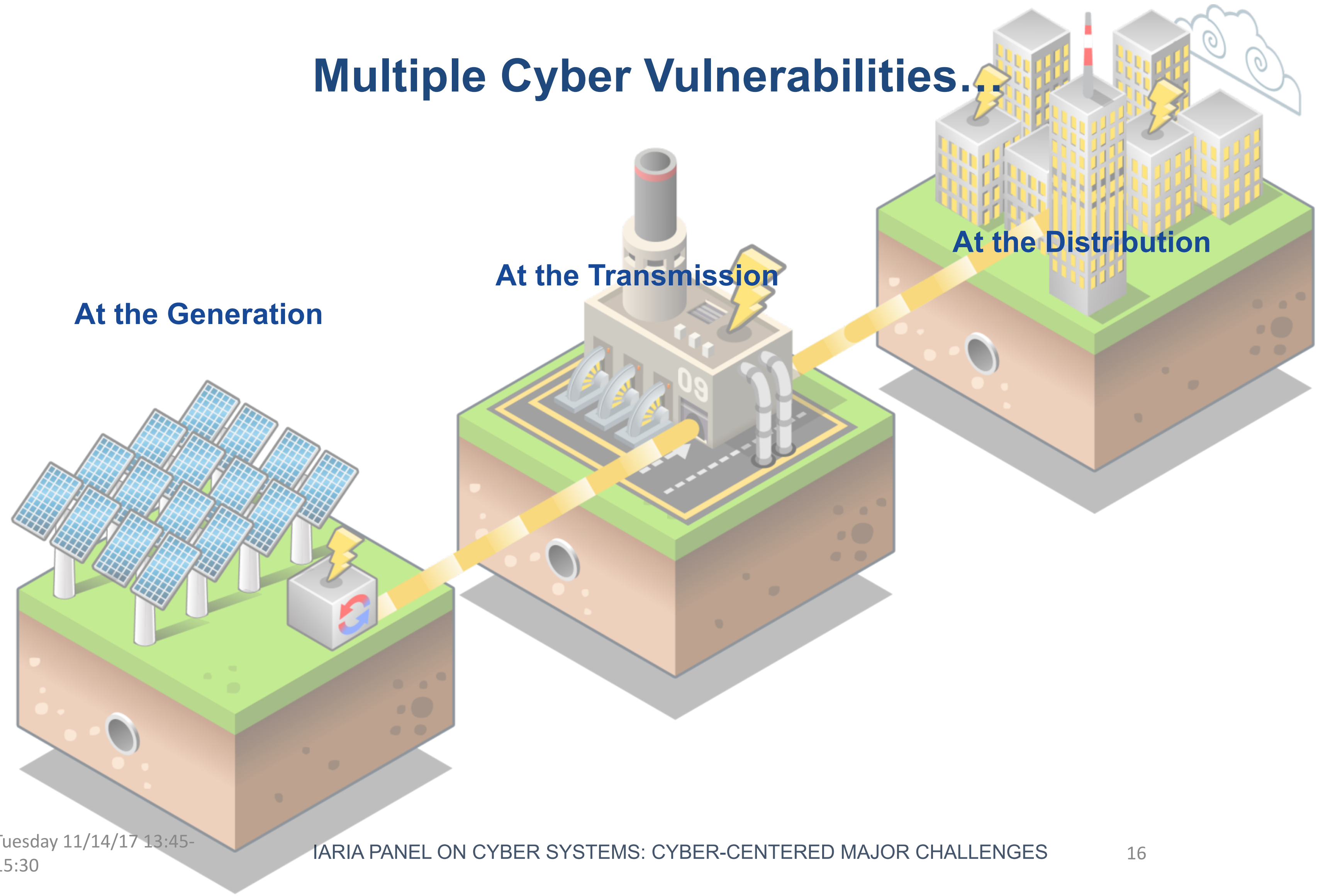
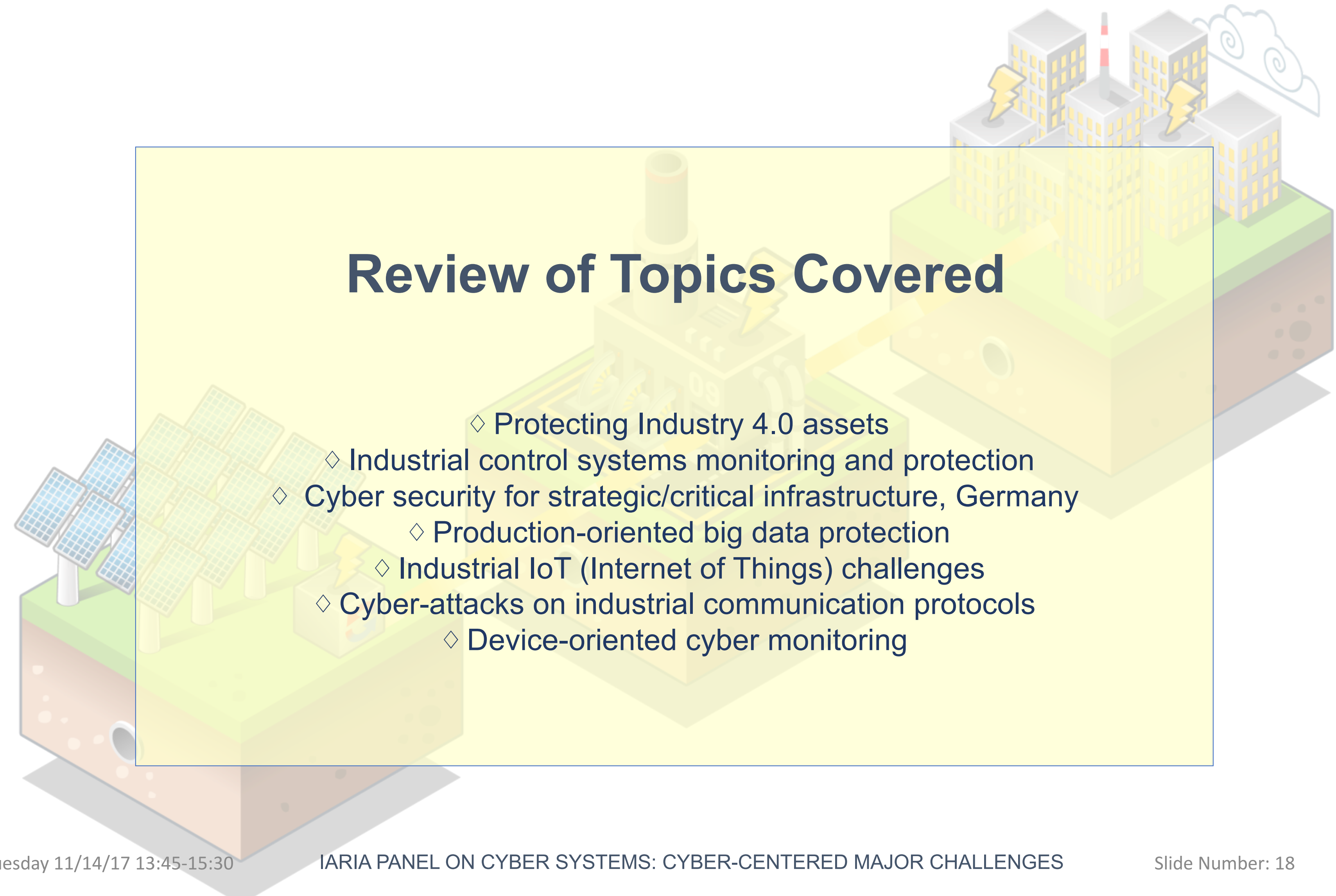


Table of Contents

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



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

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

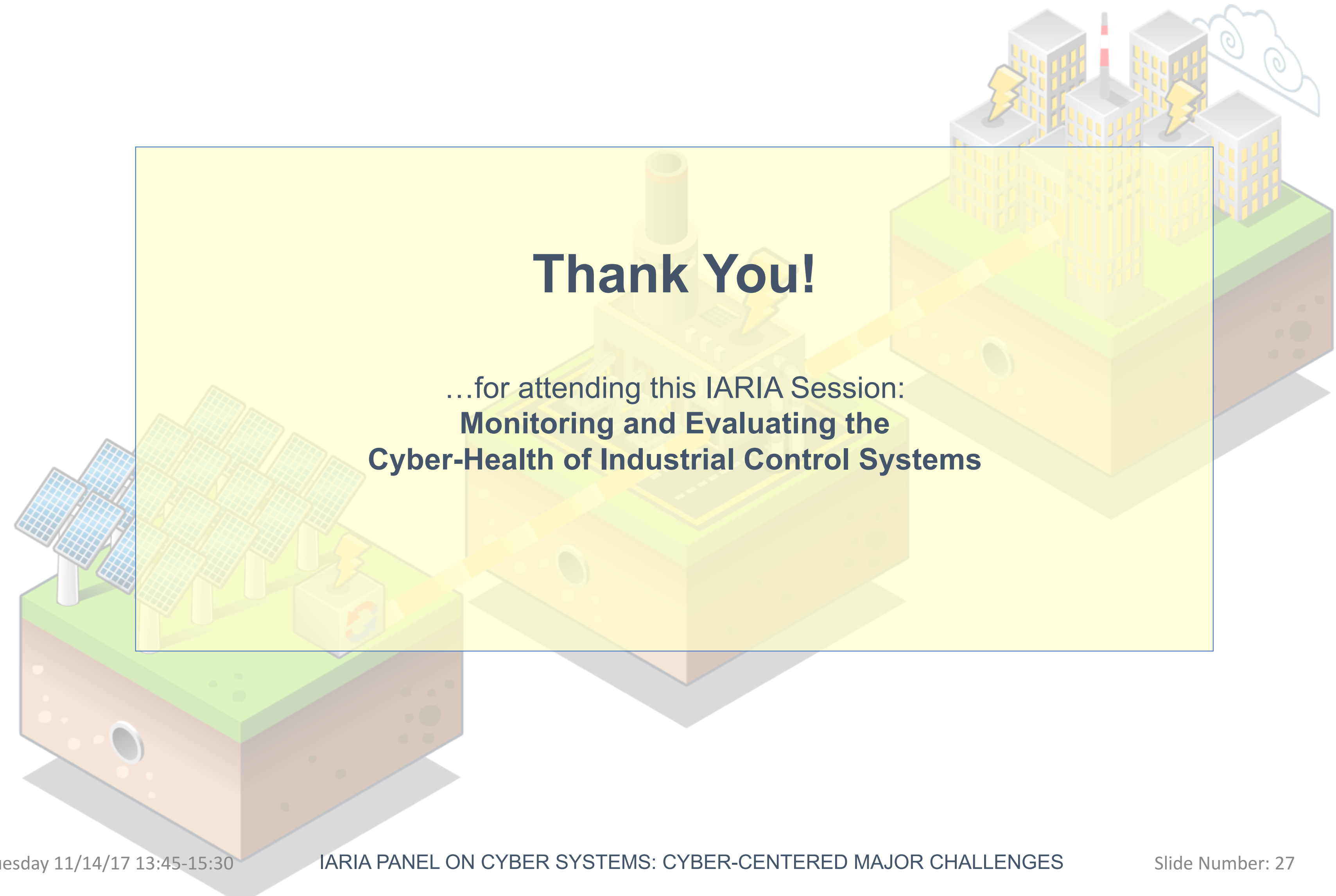
✓ ◊ Dr. Daniel Kästner, AbsInt Angewandte Informatik GmbH, Germany

Table of Contents

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

Table of Contents

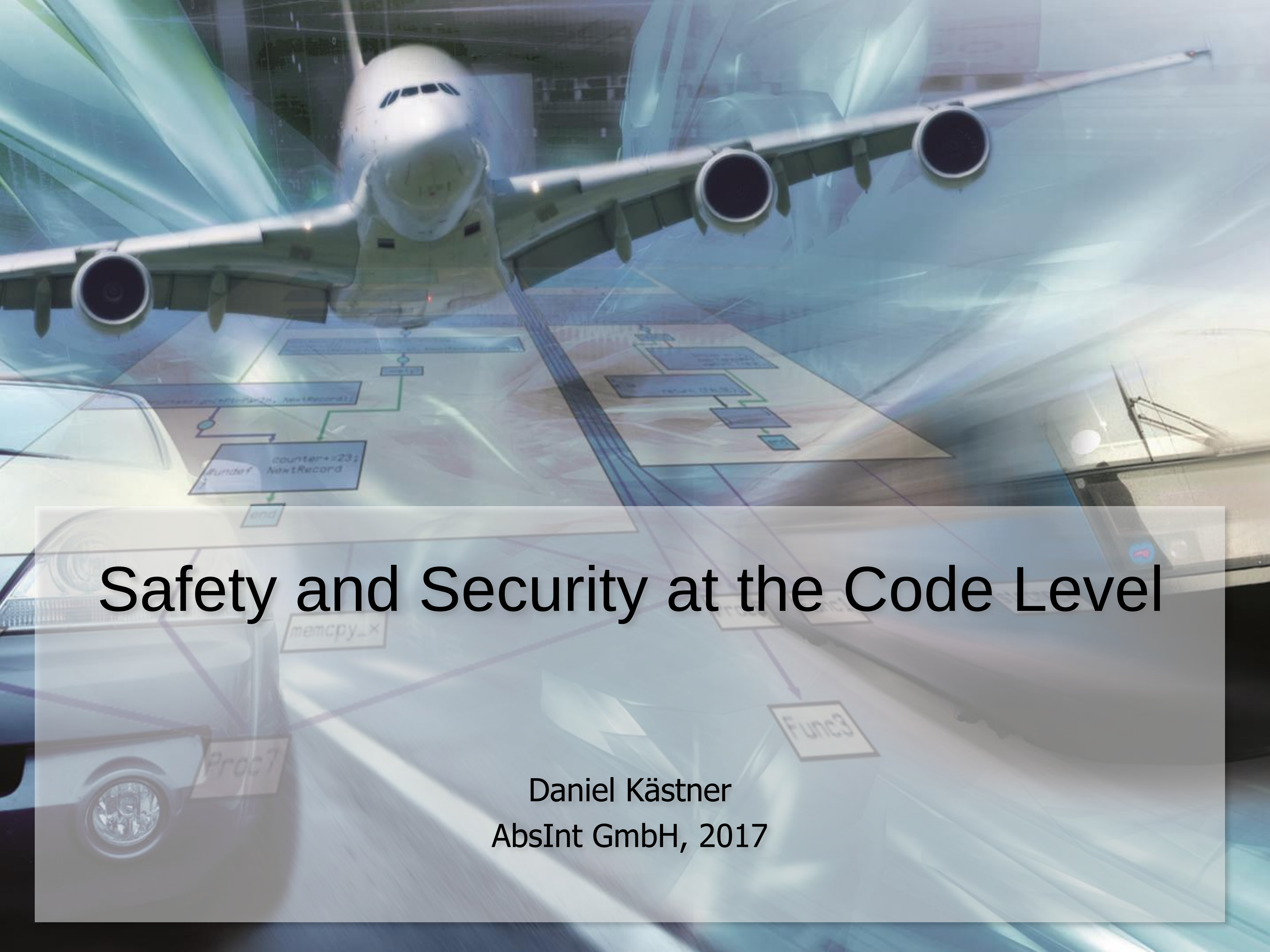
Moderated Session on Monitoring and Evaluating the Cyber-Health of Industrial Control Systems



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

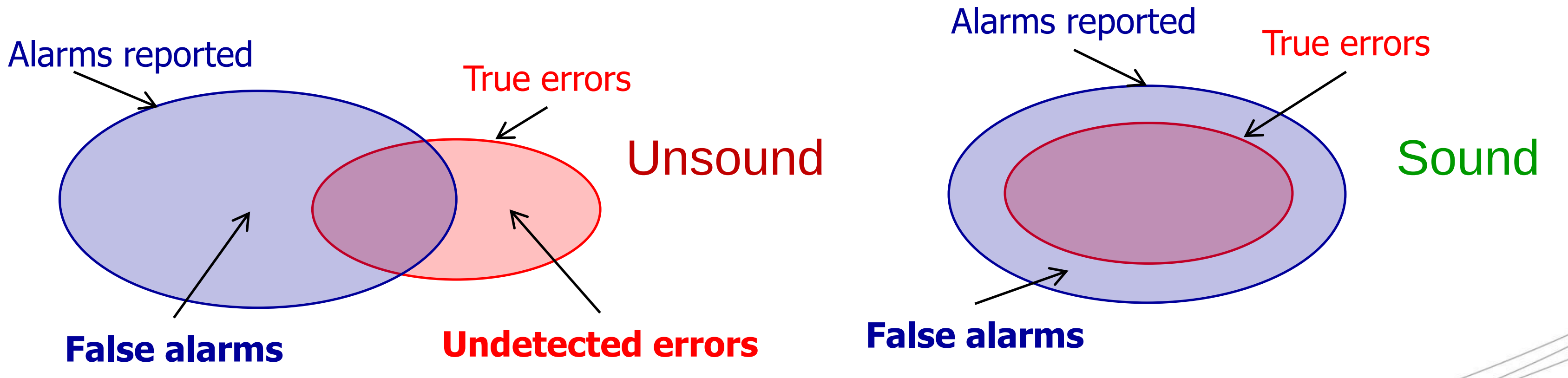
1. Stack-based buffer overflow
2. Heap-based buffer overflow
3. Further invalid pointer accesses (null, dangling, …)
4. Uninitialized memory accesses
5. Integer errors
6. Format string vulnerabilities
7. Concurrency defects

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

AbsInt

Abstract Interpretation

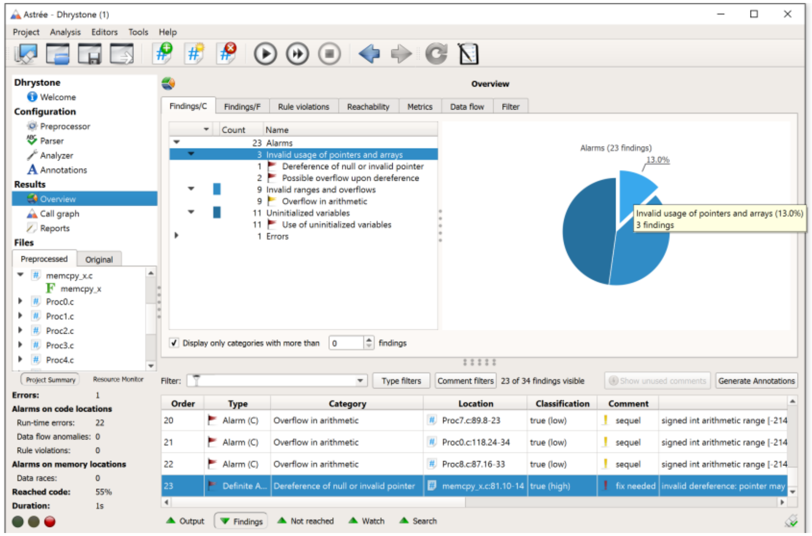
- Semantics based methodology for program analysis
- Formal method – supports correctness proofs
  - Efficiency: scales to real-life industry applications due to abstractions
  - Soundness:
    - Correctness of abstractions proven.
    - Never fail to report a defect from the class of defects under analysis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



AbsInt

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

AbsInt

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

Table 9 — Methods for software unit verification

	Methods	ASIL A	ASIL B	ASIL C	ASIL D
1a	Walk-through[a]	++	+	o	o
1b	Pair-programming	+	+	+	+
1c	Inspection[a]	+	++	++	++
1d	Semi-formal verification	+	+	++	++
1e	Formal verification	o	o	+	+
1f	Control flow analysis[b, c]	+	+	++	++
1g	Data flow analysis[b, c]	+	+	++	++
1h	Static code analysis[d]	++	++	++	++
1i	Static analyses based on abstract interpretation[e]	+	+	+	++
1j	Requirements-based test[f]	++	++	++	++
1k	Interface test	++	++	++	++
		+	+	+	++
		+	+	+	++
	...pplicable[i]		+	++	++

Table 12 — Methods for verification of software integration

	Methods	ASIL A	ASIL B	ASIL C	ASIL D
1a	Requirements-based test[a]	++	++	++	++
1b	Interface test	++	++	++	++
1c	Fault injection test[b]	+	+	++	++
1d	Resource usage test[c, d]	++	++	++	++
1e	Back-to-back comparison test between model and code, if applicable[e]	+	+	++	++
1f	Analyses of the control or data flow	+	+	++	++
1g	Static code analysis[f]	++	++	++	++
1h	Static analyses based on abstract interpretation[g]	+	+	+	+

++ ?

AbsInt

AbsInt

email: info@absint.com
http://www.absint.com

The Human Factor in Cyber Security

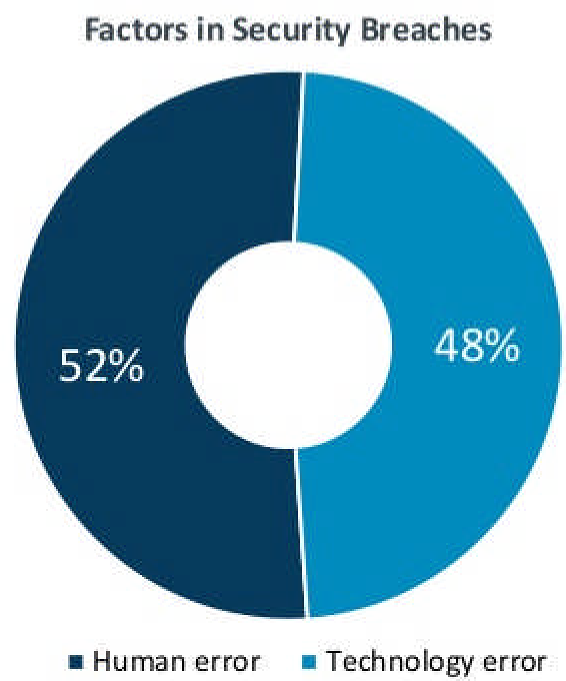
Dr Maria Bada
Global Cyber Security Capacity Centre
University of Oxford
Maria.Bada@cs.ox.ac.uk
@MariaBadaOxford

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

The Human Factor in Cyber Security



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

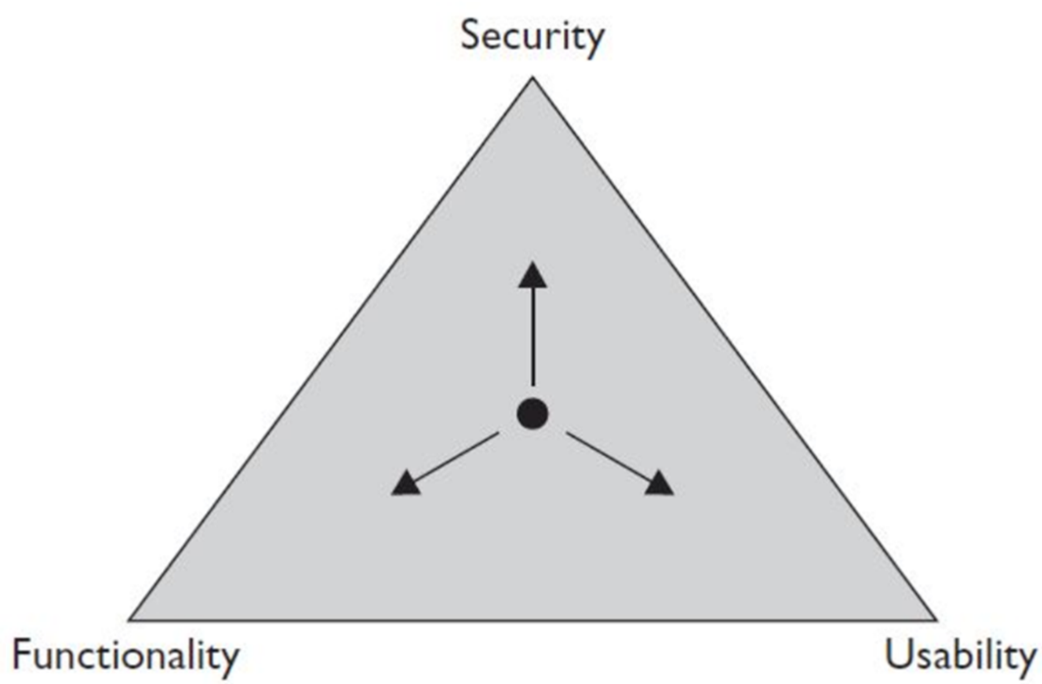
26% IT staff failure to follow policies and procedures

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

The Security, Functionality and Usability Triangle



Global
Cyber Security
Capacity Centre

OXFORD
MARTIN
SCHOOL

UNIVERSITY OF
OXFORD

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.

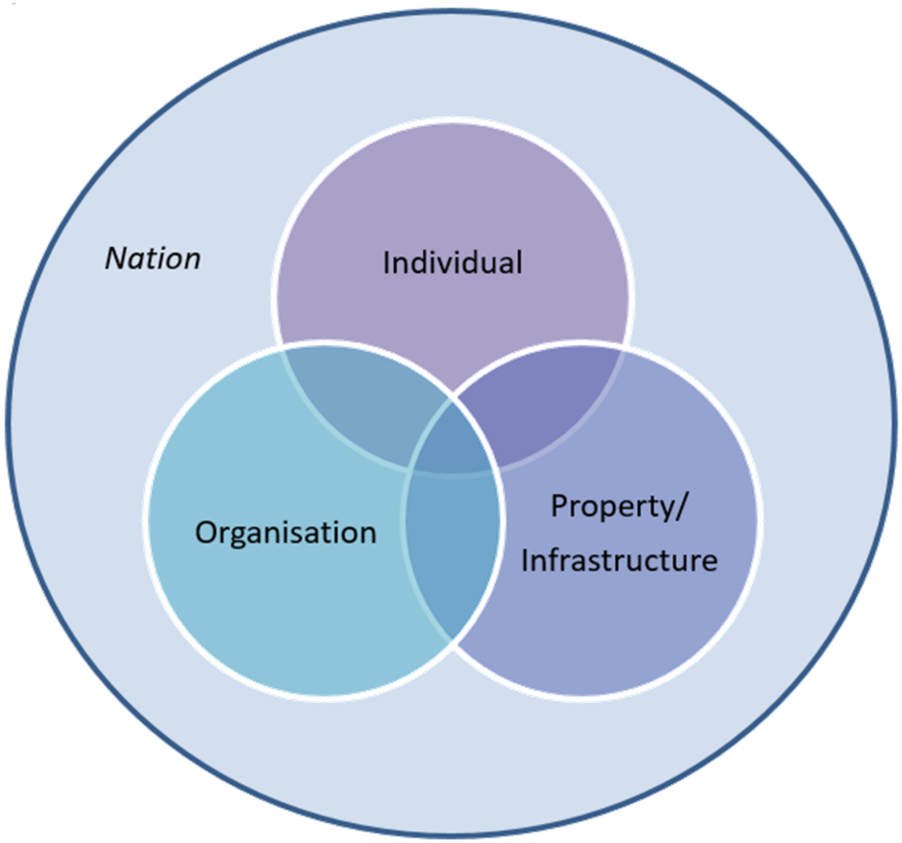
The Human Factor in Cyber Security
Lack of Awareness

Global
Cyber Security
Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

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

SIEMENS

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

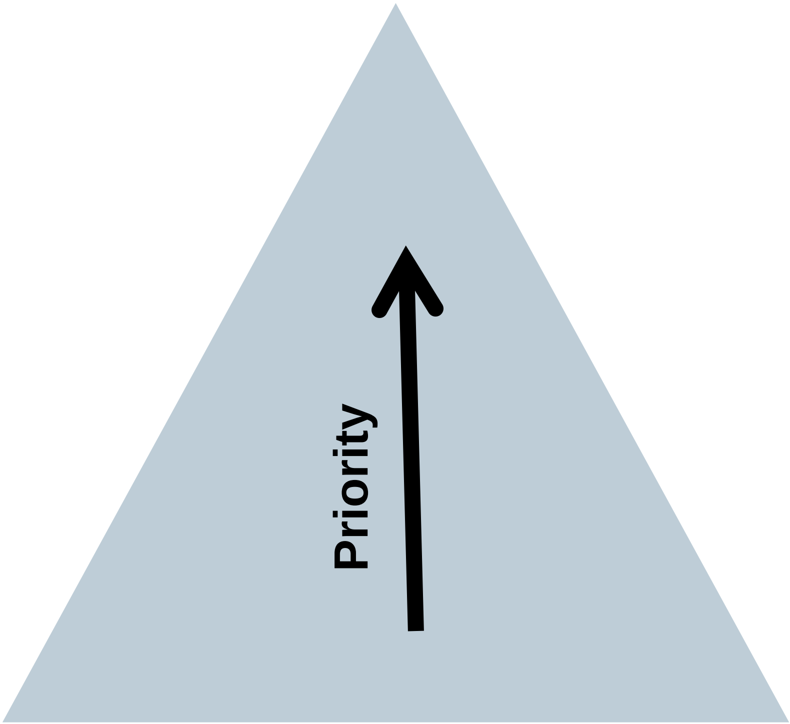
The CIA pyramid is turned upside down in industrial automation and control systems: “Protect Productivity”

Industrial Automation and Control Systems

Availability

Integrity

Confidentiality



Office IT Systems

Confidentiality

Integrity

Availability

Industrial systems and office world have different management & operational characteristics

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

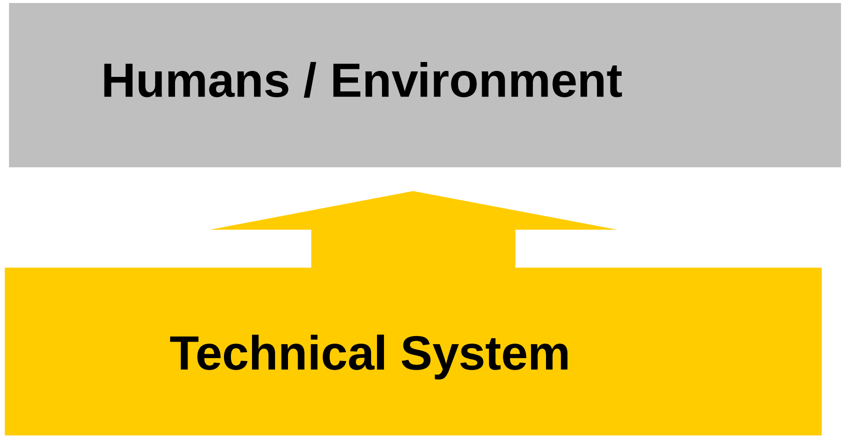
Security-by-Design is different from Safety-by-Design

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

Bundesamt für Sicherheit in der Informationstechnik
Bundesnetzagentur
Homeland Security
National Institute of Standards and Technology
ANSSI – Agence nationale de la sécurité des systèmes d'information

Asset Owner operates and maintains → **Secure operation, policies, requirements**

- ISO 27001/19
- IEC 62443-2-1
- NERC-CIP

System Integrator designs and deploys → **Design + hand over / maintain a secure solution**

- IEC 62443-2-4
- IEC 62443-3-3
- DIN VDE V0831-104
- BDEW WP

Product Supplier develops and supports → **Capabilities, documentation, secure development, support**

- IEC 62443-3-3
- IEC 62443-4-1
- IEC 62443-4-2
- BDEW WP

IEC 62443 Covers Security Management, System, and Component Level for Industrial Automation Control Systems (IACS)

SIEMENS

IEC 62443 (ISA-99)

General	Policies and procedures	System	Component
1-1 Terminology, concepts and models	2-1 Establishing an IACS security program	3-1 Security technologies for IACS	4-1 Product development requirements
1-2 Master glossary of terms and abbreviations	2-2 Operating an IACS security program	3-2 Security assurance levels for zones and conduits	4-2 Technical security requirements for IACS products
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security assurance levels	
1-5 IACS Protection Levels	2-4 Certification of IACS supplier security policies		
Definitions Metrics	Requirements to the security organization and processes of the plant owner and suppliers	Requirements to a secure system	Requirements to secure system components

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.

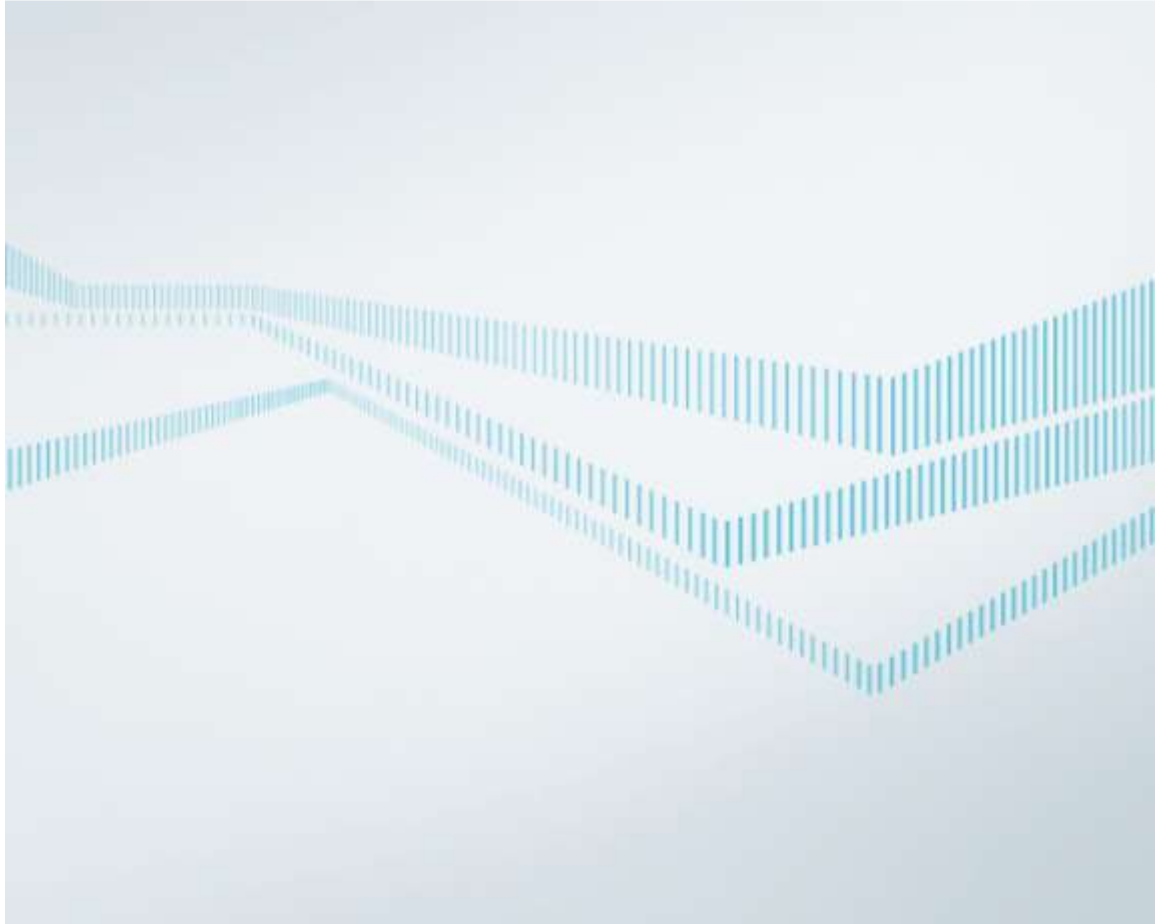
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

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

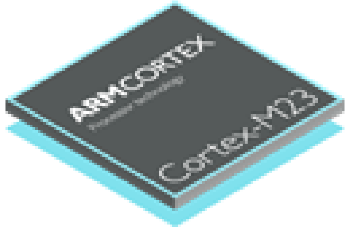
- They are similar to traditional microcontrollers (CPU, memory, input/output); plus new functions
- They are named IoT processors
- The new functions include
  - Wireless connectivity (Wi-Fi, Bluetooth Low Energy, …)
  - Security (starting with electronic design)
  - Power management and energy harvesting

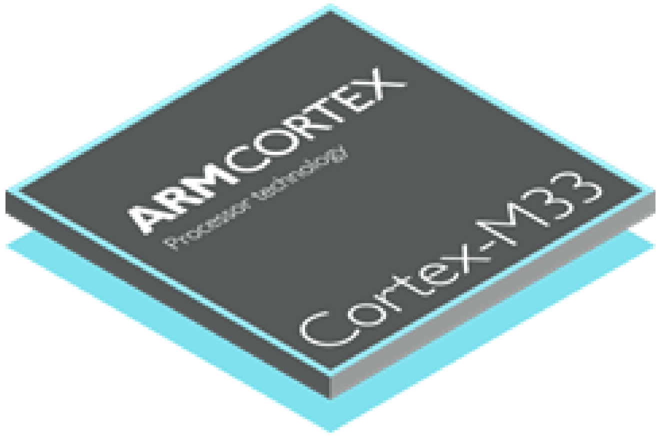
Software

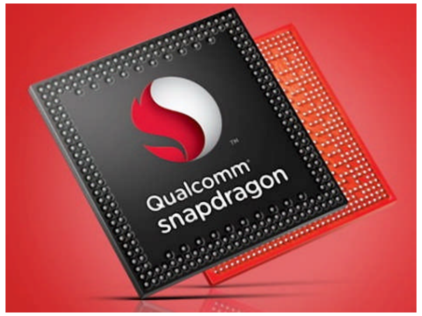
- Operating systems are now preferred for IoT devices
- They are named IoT OSes
- They are similar to operating systems in PC but smaller
  - Multitasking, memory management, file structure, device I/O
- They also have functions including
  - Supporting connectivity (software stack for Wi-Fi, Bluetooth 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

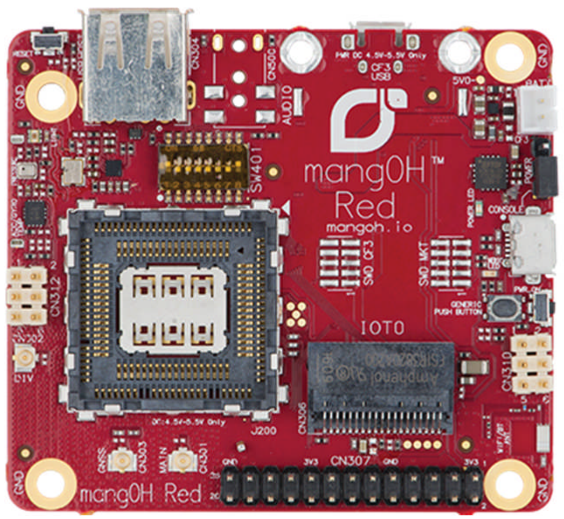


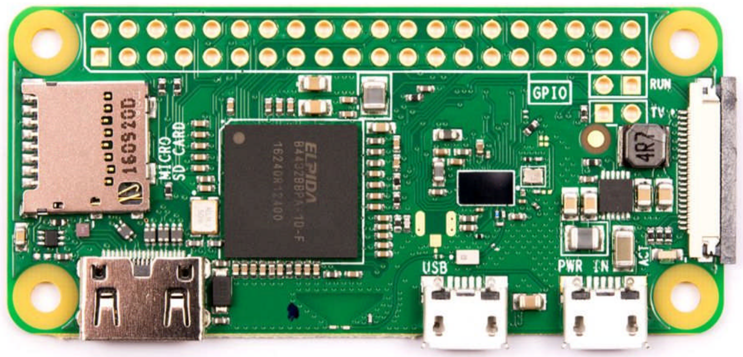




Emerging IoT Boards

- 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