

Facilitating Decision-Making Via Deep Insights

Panel on
Challenges in Cyber Services:
Tuesday 24 September 2018
15:45-17:30

Dr. Steve Chan
Moderator

Decision Engineering Analysis Laboratory

San Diego
Cambridge



Facilitating Decision-Making Via Deep Insights

Panel on
Challenges in Cyber Services:
Tuesday 24 September 2018

Anders Fongen, Norwegian Defense Cyber Academy, Norway

Daniel Kastner, AbsInt GMbH, Germany

Hannan Azhar, Canterbury Christ Church University, UK

Decision Engineering Analysis Laboratory

San Diego
Cambridge



Facilitating Decision-Making Via Deep Insights

Panel on
Challenges in Cyber Services:
Tuesday 24 September 2018

Anders Fongen, Norwegian Defense Cyber Academy, Norway

Dependency of Cyber Services: How to manage integrity requirements in a cyber supply chain? Integrity of a cyber service is much more than data integrity, it also covers the bona-fide execution of a business contract in terms of personnel training and clearance, spin-off use of data, subcontracting, availability during bankruptcy etc. I will use cases related to Huawei and Snowden, as well as examples from Norway's oil and health industry.

Decision Engineering Analysis Laboratory

San Diego
Cambridge



Facilitating Decision-Making Via Deep Insights

Panel on
Challenges in Cyber Services:
Tuesday 24 September 2018

Daniel Kastner, AbsInt GMbH, Germany

Cybersecurity in Safety-Critical Systems
Addressing cybersecurity in safety-critical systems raises specific opportunities and challenges. On the one hand, stronger assurances can be made, but on the other hand, all cybersecurity measures and services have to meet safety requirements.

Decision Engineering Analysis Laboratory

San Diego
Cambridge



Facilitating Decision-Making Via Deep Insights

Panel on
Challenges in Cyber Services:
Tuesday 24 September 2018

Hannan Azhar, Canterbury Christ Church University, UK

Human-centric cyber physical service
Does cyber-services understand human's thoughts and social context to be able to give impression of the services as a single entity rather than many independent services? Examples will be given to initiate debate on including human-layer parameters in the design of smart cyber physical services.

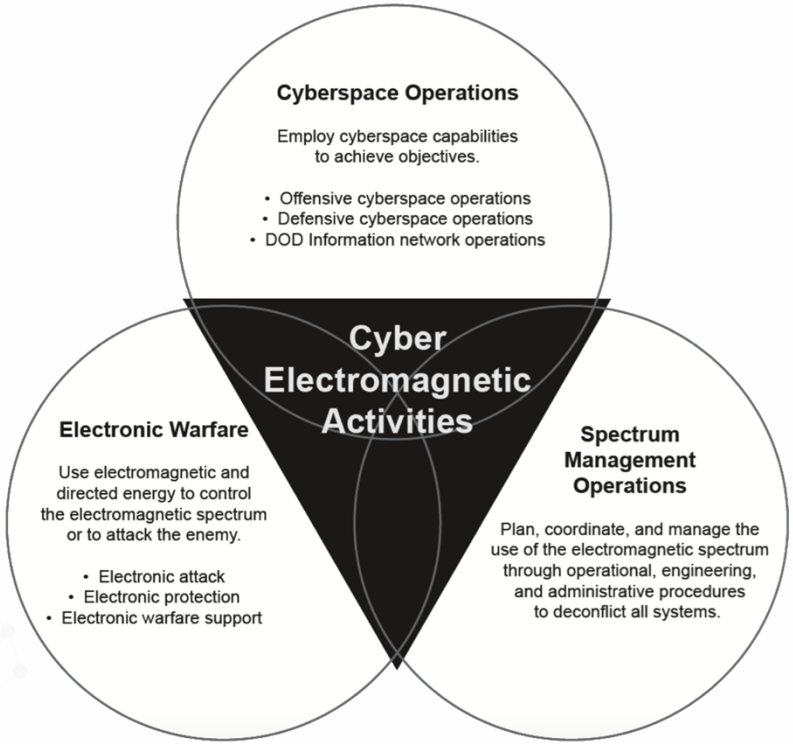
Decision Engineering Analysis Laboratory

San Diego
Cambridge



Facilitating Decision-Making Via Deep Insights

Where are you positioned?



Decision Engineering Analysis Laboratory

San Diego
Cambridge



Facilitating Decision-Making Via Deep Insights

Thank you to IARIA and all the participants of Cyber 2019.

The Fourth International Conference on
Cyber-Technologies and Cyber-Systems
September 22, 2019 to September 26, 2019 – Porto, Portugal

Decision Engineering Analysis Laboratory

San Diego
Cambridge

Neuro-security in Cyber Services

Dr Hannan Azhar

Senior Lecturer

School of Engineering, Technology and Design

Canterbury Christ Church University

Panel Discussion on Cyber Services, Cyber2019, Porto, Portugal

Use-cases

- Cyber-enabled Smart home for Neuro-rehab
- Use of BCI controlled Cyber service
- Targeted Advertisement
  - Emotional recognition using sensors
  - Realtime access to Person's interest, emotional data
- Emotional data for training for better performance

Underlying Technology

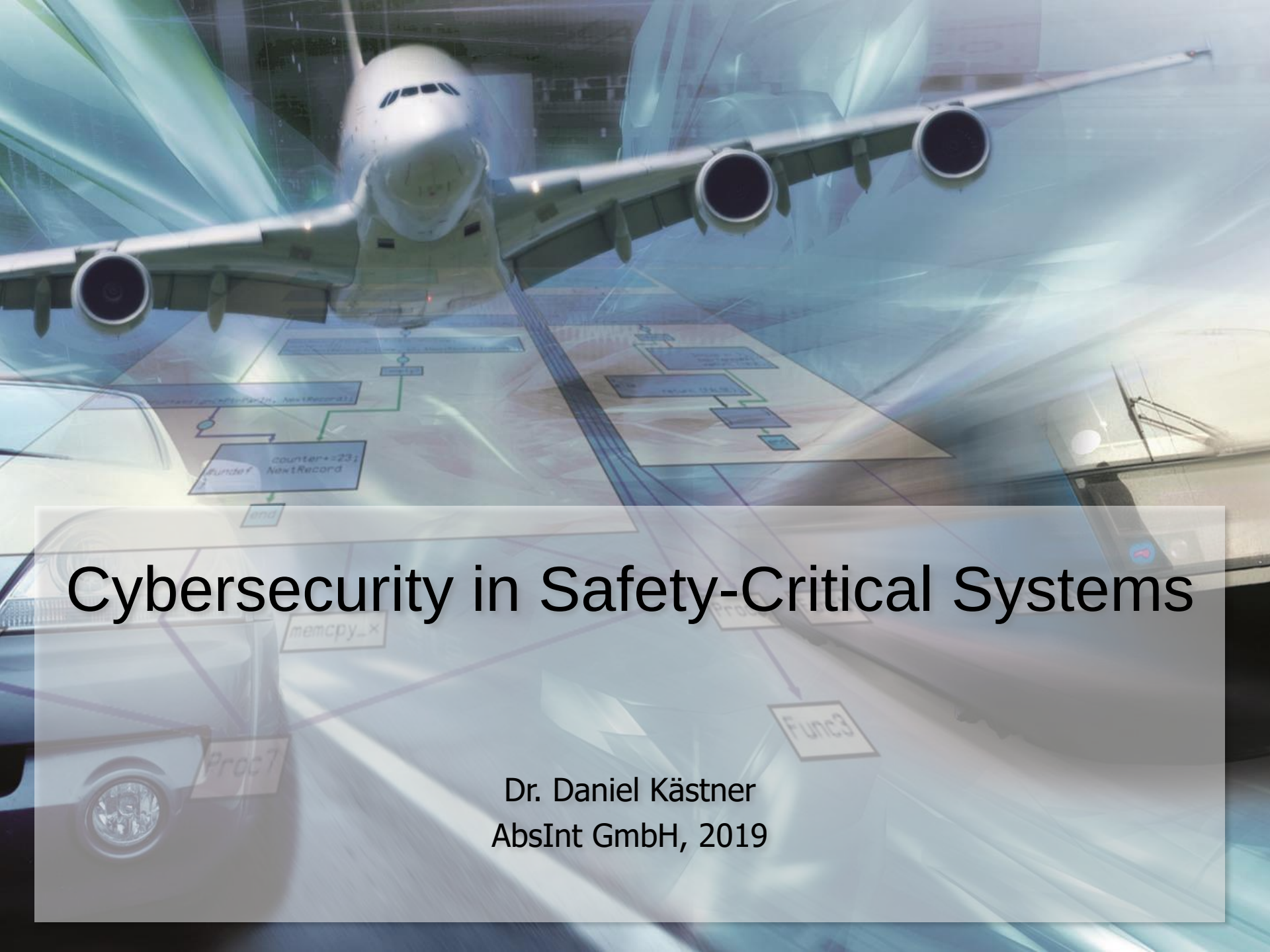
- Oddball paradigm
  - BCI application to control robotic arm
- Facial Expression detection Software
- Cost effective reliable devices
- Analysis of EEG signal
- %BPM change
- Social assessment of elderly

Security Issues

- Examples of physical and emotional harm
- Example of compromised BCI system
- Brain Malware
  - Hijak of existing components
  - Side channel attack
  - Use of malicious stimuli in overt of subliminal way

Neuro-security in cyber services

- Inter-disciplinary effort
- Use of laws and policies
- Visibility of security level across products
  - E.g. https://www.bbc.co.uk/news/technology-48106582
- Standardisation to secure BCI systems
- Developers in compliance



Cybersecurity in Safety-Critical Systems

Dr. Daniel Kästner
AbsInt GmbH, 2019

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

- Observations
  - Vulnerabilities often based on defects that might cause system to malfunction by itself ⇨ Safety/Security Link (“Common Cause”)
  - Increasingly complex software systems (autonomy, connectivity, …) pose verification challenges
  - Increasing connectivity of embedded devices (automotive, medical) opens up new level of privacy concerns

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.

- But: existence of vulnerabilities unavoidable
  - Spectre/Meltdown, ORC attacks

Discussion

- In safety-critical systems proving the absence of (some) code-level defects is possible
  - In security-relevant safety-critical systems the absence of (some) code-level vulnerabilities can be shown
- Trend to increasing connectivity and software complexity could endanger established level of safety
  - Non-safety-critical programming concepts (typical C++ usage)
  - Heterogeneous programming language environments
  - Neuronal networks, deep learning, …
- New threats: side channel attacks, …
- What is acceptable level of safety and cybersecurity?
- Should we give up deterministic safety (security) for more connectivity / more ambitious system scope?
- Are there specific services for safety and security properties of embedded code?

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

Dependency of Cyber Services:

How to manage *service integrity* requirements in a cyber supply chain?

Dr. Anders Fongen
Norwegian Cyber Defence Academy

What is *Service Integrity?*

A cyber service delivered in observation of:

- Expectations
- Service contract (Service Level Agreement, SLA)
- Business ethics and legislation
- Good practice

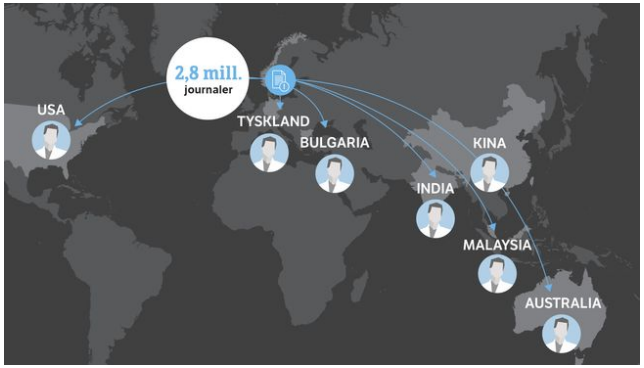
Results in a *bona-fide* execution of the service interface

Cyber services are delivered:

- From in-house equipment and personnel
- Free online services
- Contractual services, subject to agreements and protected by law
  How is service integrity protected during
  - Bankruptcy
  - Malware attack
  - Misuse by disloyal personnel

Examples

- Huawei products in 4G networks
  - Can we trust the software not to contain back doors for intelligence and cyber attacks?
- Edward Snowden
  - How can DoD trust Booz Allen Hamilton to suuply only loyal personnel?
- GPS, free but owned by one single government
- Norwegian Oil Refinery 2014 (Statoil, now Equinor)
  - Operation outsourced to India,
    a mistake stopped the entire plant
- Norwegian patient journals (2017)
  - system operation outsourced to Bulgaria and Asia
  - unauthorized personnel had access to 2.8 mill journals



Can we provide *Integrity Attestations?*

- A cryptographic document bound to a server state, able to prove:
  - clean, approved service software
  - approved software/hardware platform
  - authorized system personnel
  - location of data storage
  - supervision and control over subcontractors
- Client can validate it (like a public key certificate)
- Trusted Platform Module (TPM)
  - Sealed keys and certificates
- Trusted Execution Environment (TEE)
  - Intel *Trusted Execution Technology*
  - ARM *TrustZone*
  - etc.
- Requires “openness” in OS to extend the trust chain from HW/BIOS/OS to application software

Thank you for your attention!

Suggestions, thoughts?