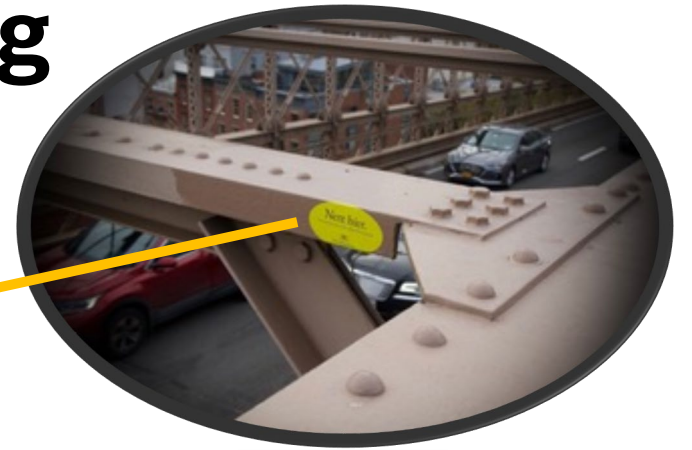


Driven by the future: Strategic Dialogue for the Automotive Sector in Baden-Württemberg





The digital car of the future – cybersecurity risks and opportunities

Digital Trust as new Approach to AI Governance

Dr. Christoph Peylo, SVP Prj. Digital Trust

Foundations of Digital Trust

As trust in IoT is broken, legislation is about shifting gears



“Unsecurable”

Chris Inglis (2010), Former Deputy Director
National Security Agency



“Indefensible”

Gen. Keith Alexander (2011), Former Director
NSA und Commander of the United States
Cyber Command



“Hopeless”

Ron Rivest (2012), Co-Inventor of RSA-Crypto
Systems, Turing Award (2002)



“Lousy IoT Security”

Bruce Schneier (2019) Writer, fellow and
lecturer at Harvard's Kennedy School, board
member of Electronic Frontier Foundation

- EU commission adopts HLEG¹ view of trustworthy, e.g., lawful, ethical, robust (which includes security and safety) AI in its proposal for AI regulation.
- Responsible AI requested in AI-strategy of federal government.
- Several initiatives on AI and Data handling on EU level, including a Cyber Resilience Act and revision of NIS2².
- IT SiG³ strengthened role of BSI. BSI is now about setting standards for cloud-based AI and standards for AI certification to achieve trustworthiness.
- StVG⁴ asks for accident prevention systems that can decide on by taking fundamental values into account.
- 1: High Level Expert Group, 2: *Directive on Security of Network and Information Systems* 3: IT Sicherheitsgesetz 4: Straßenverkehrsgesetz

As trust in IoT system is shaken since several years, legislation start now to enforce higher degrees of security and trustworthiness.

Digital Trust as new Approach to AI Governance

Motivation for Digital Trust

There is no “natural trust” in the Digital World

- Trust needs **assurance by legitimation** or by **experience over time**. Both needs structure.
- **Digital World** is under **constant development and change**.
- It is an extremely brittle **environment with low inherent trust**.



Digital Trust has to be actively established


- As **trust in IoT system is shaken**, legislation starts now to enforce higher degrees of security and trustworthiness.
- Legislation and standardization are formal ways to express **expectations of society**.
- Digital Trust has to take the **expectations of customers** during **the whole life cycle** of products into account.
- Context and scope of “Trust” have to be established individually and transparently for each digital product.


Digital Trust is the **corresponding counterpart** of core **value propositions of the non-digital world**.

Foundations of Digital Trust



Challenges imposed by AI


Imperfect AI leading to unethical behavior





Recognized as





Google Übersetzer


Deutsch Englisch Türkisch Sprache erkennen

He is nice
She is smart
He is a nurse
She is a doctor

Türkisch Englisch

O güzel
O akıllı
O bir hemşire
O bir doktor



Intended unethical behavior



Jeremy Corbyn urges voters to back Boris John... Link kopier...

Boris Johnson tells "people's cabinet" to work "24 hours a day" The Telegraph • 47.434 Aufrufe

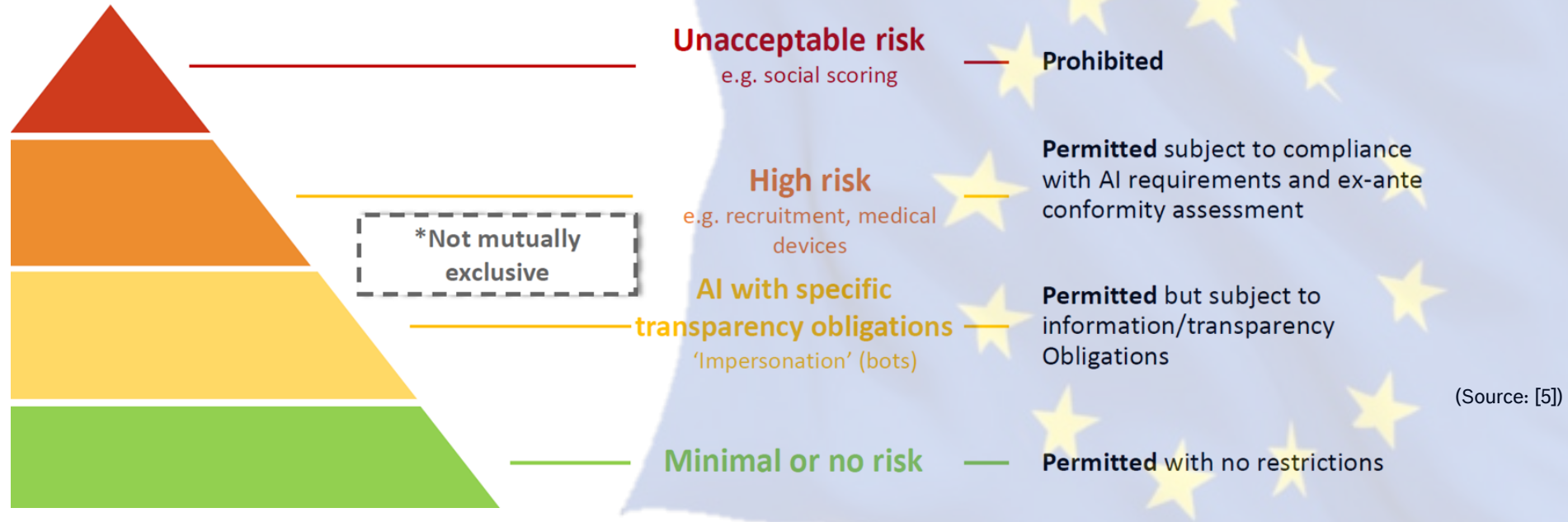
3:20



European Commission proposal for AI Regulation in April 2021 applies a risk-based approach to regulation, where both, the term of risk and the definition of AI has been widened.

Efforts for Re-Establishing Trust

AIA's Risk Model



European Commission proposal for AI Regulation in April 2021 applies a risk-based approach to regulation.

Digital Trust as new Approach to AI Governance

A Label for Digital Trust – „easy to understand“

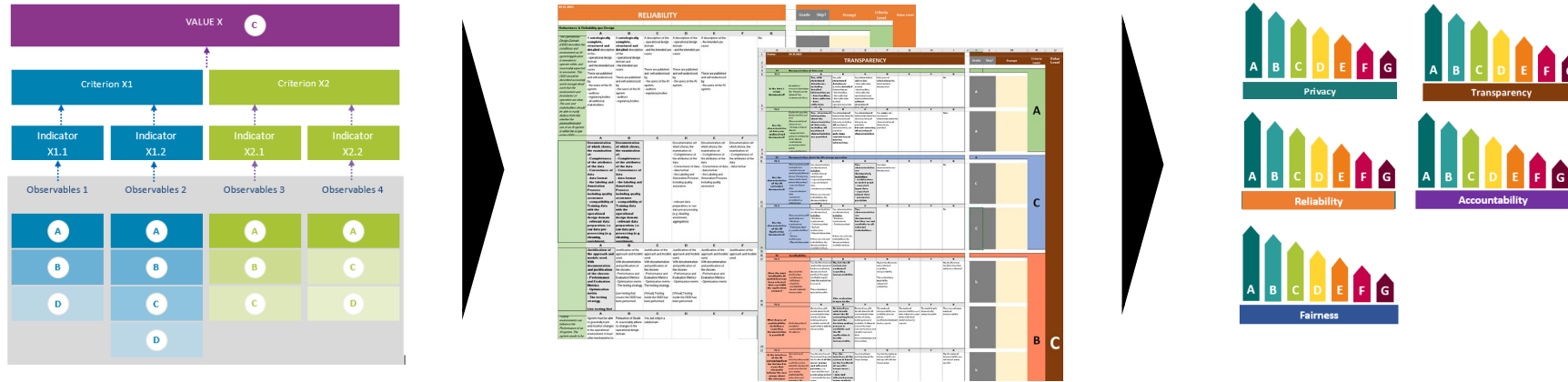


- Bosch and Siemens developed with VDE and partners from industry a VDE SPEC for an **AI trust label**.
- Dimensions like “transparency, privacy, fairness, ...” as important aspects for trust can be made **concrete and tangible**.
- This label can be assigned to a product in both **B2C and B2B** context.
- Thus, **customers can decide about the degree of “Digital Trust”** they need.
- This effort is currently being developed as European standard that will comply with the AI Act.

After completion and acceptance of the Digital Trust Label by the EU, this could be an easy to understand way for consumer & customer - if a solution/ product complies with the AI legal regulations.

Digital Trust as new Approach to AI Governance

Criteria-based model as foundation for Digital Trust



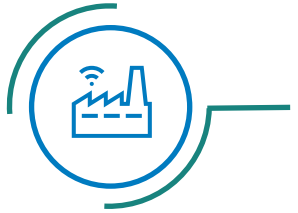
The Value-Criterion-Indicator-Observable (VCIO) approach is based on the assumption that

- Each **value** is based on a set of **criteria**,
- There is a set of **indicators** if the criteria are met,
- **Indicators** have to be supported by **observable** facts, processes or activities.
- The overall rating is the aggregated result of how values are reflected in observable activities.

This standard gives transparency, whether a product adheres to specific values and can be trusted.

Digital Trust as new Approach to AI Governance

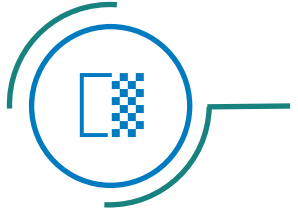
AI allows unprecedented efficiency gains



Focus: Industrial Application of Artificial Intelligence



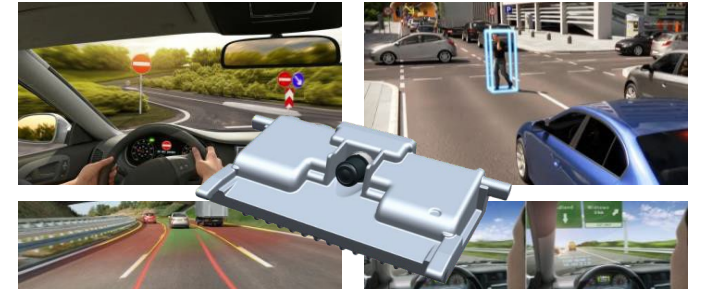
Implementation in **physical products** and **machines**



Hybrid models: Combination of **model-based** and **data-driven approaches**



Industrial AI is **safe, secure, robust** and **explainable**



As trust in IoT system is shaken since several years, legislation start now to enforce higher degrees of security and trustworthiness.



**Thanks for your kind
attention**