KI für I4.0 Sicherheit

Panel auf der it-sa 2019, organisiert von BITKOM

(Dr. Detlef Houdeau, Infineon Technologies AG)

Plattform Industrie 4.0, Kurzvorstellung

Geschäftsstelle gefördert von **BMWi** und **BMBF**

AG3: Sicherheit vernetzter Systeme

UAG: KI für I4.0 Sicherheit

Erste Publikation zur **HMI 2019**

Zweites Whitepaper in 12/2018 gestartet

Zieltermin für Veröffentlichung: **Digital Gipfel** (28.10.19)

Sprache: Deutsch

Plattform Industrie 4.0: KI für I4.0 Sicherheit

Drei Ziele sind zu unterscheiden:

- KI-Nutzung bei Cyberangriffen (***Angreifer***)
- KI-Nutzung zur Cyberabwehr (***Verteidiger***)
- Cyberangriffe, um KI-Systeme zu manipulieren (***Angreifer***)

Plattform Industrie 4.0: KI für I4.0 Sicherheit

Inhalt des neuen Whitepaper:

- Einleitung: **Trainierte** und **vortrainierte** Systeme
- **Erklärbarkeit** von KI-Entscheidungen
  - Notwendigkeit, Komplexität, Forschungsansätze, Beispiele
- **Täuschung** von KI durch gegnerische Beispiele
  - MNIST-Beispiel
- **Sicherheitsrisiko** bedingt durch **Architekturen** und **Anwendungen**
  - Statisch versus dynamische Anwendungen
  - Geschlossene versus offene Anwendungen
  - Sicherheitsrisiken mit Beispielen
- Begriffsbestimmungen