Kurzbeschreibung für den ISIS-Kurs

- Blockchain für die vernetzte Automatisierungstechnik (Axel Vick)
  - » Ziel: Absicherung automatisierungstechnischer Daten über kryptografische Methoden
  - » Aufgabe: Analyse von relevanten Automatisierungskomponenten wie (Soft-)SPS, Embedded-PCs, Sensoren, Aktoren, usw.
  - » Analyse von relevanten Ausführungsumgebungen und Kommunikationsinfrastrukturen wie VMs, Container, Feldbusse, OPC UA, TSN, usw.
  - » Analyse von etablierten und aufkommenden Algorithmen zur Konsensbildung und Dokumentation (aka Blockchain)
  - » Evaluation der Aufwände, Zuverlässigkeit, Echtzeitfähigkeit, usw.
  - » Gruppengröße: *min. 2, max. 3*
  - » Voraussetzungen: Fundierte Programmierkenntnisse (C/C++, Python), Grundkenntnisse in Automatisierungstechnik, Kenntnisse und Interesse in Kryptografie und Informationssicherheit

Blockchain für die vernetzte Automatisierungstechnik

Axel Vick

Fachgebiet Industrielle Automatisierungstechnik

Blockchain für die vernetzte Automatisierungstechnik

Ziel: Absicherung automatisierungstechnischer Daten über kryptografische Methoden

- Problemstellung
  - Zunehmende Modularisierung, Virtualisierung und Vernetzung von automatisierungstechnischen Prozessen und Steuerungstechnik erfordert häufig die Datenkommunikation über vertrauenswürdige Netzwerkgrenzen hinweg.
  - Beispiel: Ein Fabrikbetreiber möchte KI-Methoden eines Softwareherstellers nutzen, der diese in einer Public Cloud als Web Service anbietet.
  - Während der Produktion muss der Betreiber darauf vertrauen, dass immer der korrekte Algorithmus auf dem richtigen Rechner angesprochen wird, seine eigenen Prozessdaten sicher zum Web-Service gelangen, die Antwort auf dem Rückweg nicht manipuliert wird und schließlich die (Steuerungs-)Daten nicht zu einer Beschädigung der Maschinen und Anlagen führen
- Idee
  - Der Datenverkehr wird mittels kryptografischer Methoden abgesichert und fälschungssicher dokumentiert.
  - Annahme: Blockchains bieten diese Funktionalität

Blockchain für die vernetzte Automatisierungstechnik (2)

Ziel: Absicherung automatisierungstechnischer Daten über kryptografische Methoden

Aufgaben

- Analyse von relevanten Automatisierungskomponenten
  - (Soft-)SPS, Embedded-PCs, Sensoren, Aktoren, usw.
- Analyse von relevanten Ausführungsumgebungen und Kommunikationsinfrastrukturen
  - VMs, Container, Feldbusse, OPC UA, TSN, usw.
- Analyse von etablierten und aufkommenden Algorithmen zur Konsensbildung und Dokumentation
  - Gegenüberstellen von PoW, PoS, PoA, PoB Mechanismen, Smart Contracts usw. und Auswahl geeigneter Kandidaten
- Implementierung mind. einer abgesicherten Kommunikation zwischen zwei Endpunkten
- Evaluation
  - Machbarkeit, Aufwände, Zuverlässigkeit, Echtzeitfähigkeit, usw.

Voraussetzungen

- Gruppengröße: 2-3 Studierende
- Vorkenntnisse: Fundierte Programmierkenntnisse (C/C++, Python), Grundkenntnisse in Automatisierungstechnik, Kenntnisse und Interesse in Kryptografie und Informationssicherheit