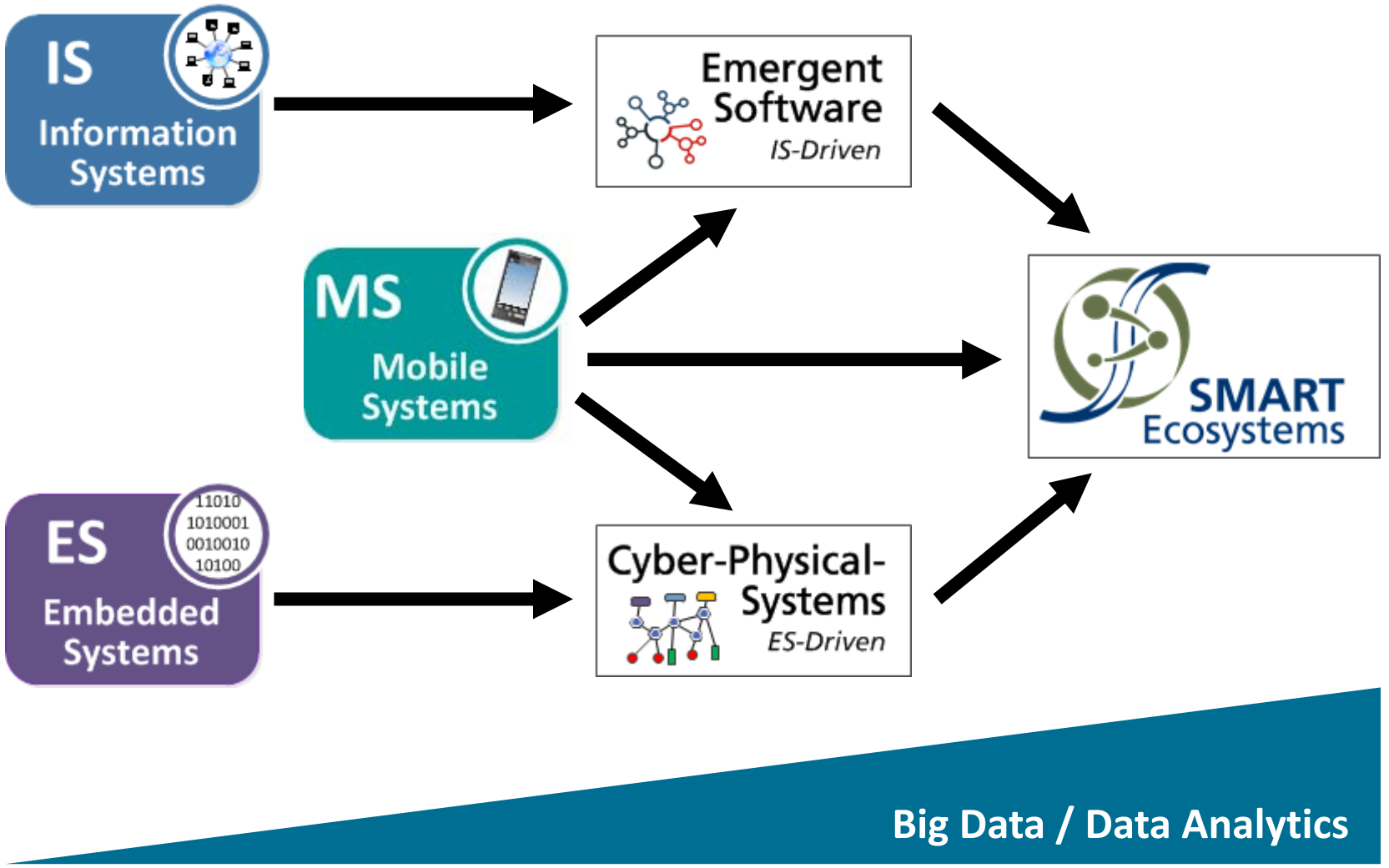
Datensouveränität für die Energiewende - Impulsvortrag

Joerg Doerr, 28.6.2017
joerg.doerr@iese.fraunhofer.de

Fraunhofer
IESE

Megatrend Integration ES/IS → Smart Ecosystems



„Daten sind das neue Gold“

„Daten sind das neue Öl“

„Daten sind die neue Währung“

„Daten sind der vierte Produktionsfaktor“

→ Daten sind auch von besonderer Relevanz für die Energiewende

Nur wer die Daten
a) nutzen darf
b) adäquat schützt,
kann sie als Produktionsfaktor
dauerhaft nutzbar machen!

→ Endnutzer und Geschäftspartner stimmen der Nutzung eher zu, wenn Datensouveränität und Kontrolle über die Daten gewährleistet bleibt.

Unterschiede im Schutz der Daten im Zuge der Datensouveränität

Fort Knox-Lösung

- Schutz der Infrastruktur, aber nicht des Inhalts selbst
- sicher
- unflexibel

Verteilte Nutzungskontrolle

- Zugang über spezifische, verteilte Zugangspunkte
- Sicherheitskontrolle bei jeder Nutzung
- Daten selbst werden geschützt
- Flexibel änderbar – je Datum/Nutzung/ Kontext

Tyische Ziele verteilter Datennutzungskontrolle

- Datennutzungskontrolle ermöglicht Applikationen, die Verwendung von Daten gezielt und dynamisch (zur Laufzeit) zu steuern und zu kontrollieren
- *„Daten werden nach Verwendung automatisch gelöscht.“*
- *„Die Daten meiner Smart Home Anwendungen dürfen nur für die Optimierung meines Energieverbrauchs genutzt werden.*
- *„Die Daten meiner Photovoltaik-anlage dürfen nur für den Zweck der Effizienzoptimierung analysiert werden.“*
- Datennutzungskontrolle reduziert Risiken, auch wenn Zugangskontrollmechanismen versagen.

  "In 10 min dürfen nicht mehr als 100 Datensätze gelesen werden.“

  Datennutzungskontrolle ersetzt Zugangskontrolle nicht bzw. Zugriffsschutzmechanismen, sondern erweitert diese um zusätzliche Steuerungs- und Kontrollmöglichkeiten!

Schützenswerte Daten

Business data
Process data
Product data

Intellectual property

Customer data
Employee data
Contractor data
Personal data

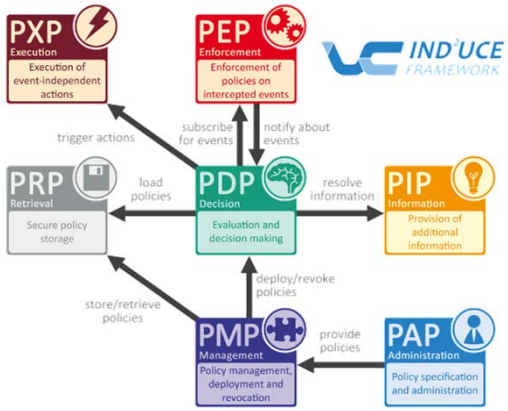
Fraunhofer IESE

IND²UCE Framework

EARTO IMPACT DELIVERED

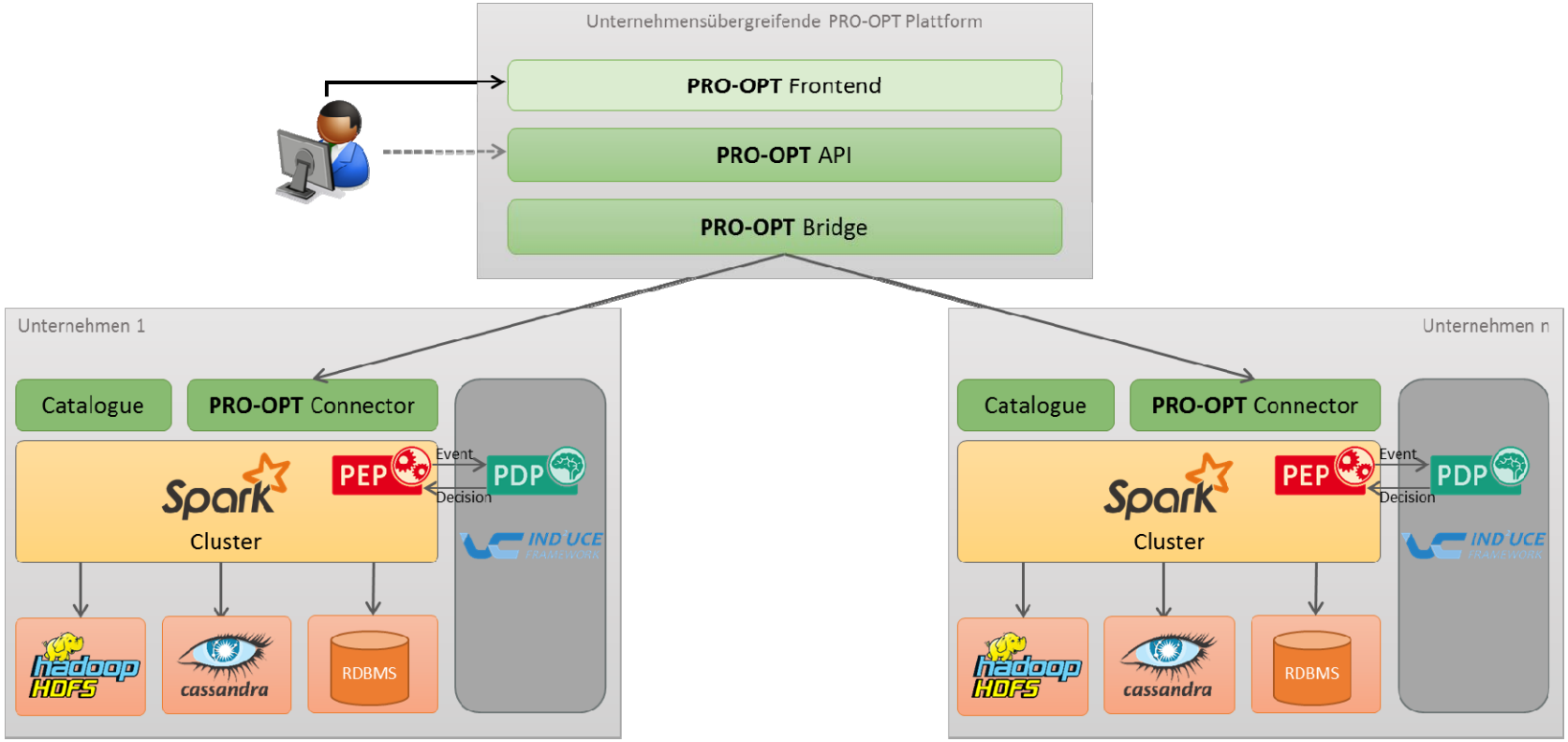
2014 Innovation Prize Winner

- Das IND²UCE Framework (INtegrated Distributed Data Usage Control Enforcement) stellt alle notwendigen Komponenten zur Implementierung von Datennutzungskontrolle bereit
- Das Framework wurde in unterschiedlichsten Umgebungen implementiert und kann am Fraunhofer IESE im Data Usage Control Lab evaluiert werden.



Fraunhofer IESE

Datensouveränität am Beispiel Automotive / Produktion: das BMWI PRO-OPT Projekt



Nutzungsmöglichkeiten im Energiebereich

- Das ***Vertrauensverhältnis zum Endverbraucher*** kann über IND²UCE unterstützt werden
  - Endverbraucher kann im Zuge seiner Datensouveränität ***einfach*** Nutzungsrichtlinien spezifizieren (wenn er will!)
- ***Unternehmen*** können im Energie-ökosystem ***wechselseitig Daten vertrauensvoll für unterschiedlichste Geschäftsmodelle*** verwenden, z.B.:
  - Verschiedenste Datenanalysen können ermöglicht werden
  - Unternehmen spezifizieren Richtlinien
  - Lokale Energieeinspeiser können spezifizieren, wer welche Erzeugungsdaten nutzen darf
  - „Energiemuster“ können per Richtlinien analog zu Rezepturen in der Produktion geschützt werden (Schutz von IP, Pirateriesschutz)

Zusammenfassung

- Daten sind ein Kernbaustein zukünftiger Geschäftsmodelle, auch im Energiesegment! ***Verteilte Datennutzungskontrolle*** ermöglicht neue Geschäftsmodelle die durch intensive Datennutzung geprägt sind
- Durch Datennutzungskontrolle wird der ***Nutzwert der Daten signifikant erhöht***
- Datennutzungskontrolle ermöglicht der Person, die über die Datennutzung bestimmen darf die **Kontrolle über die Daten** zu behalten → ***Datensouveränität*** bleibt erhalten / wird ermöglicht
- Datennutzungskontrolle trägt somit maßgeblich zum **Vertrauen bzgl. der Datennutzung** bei