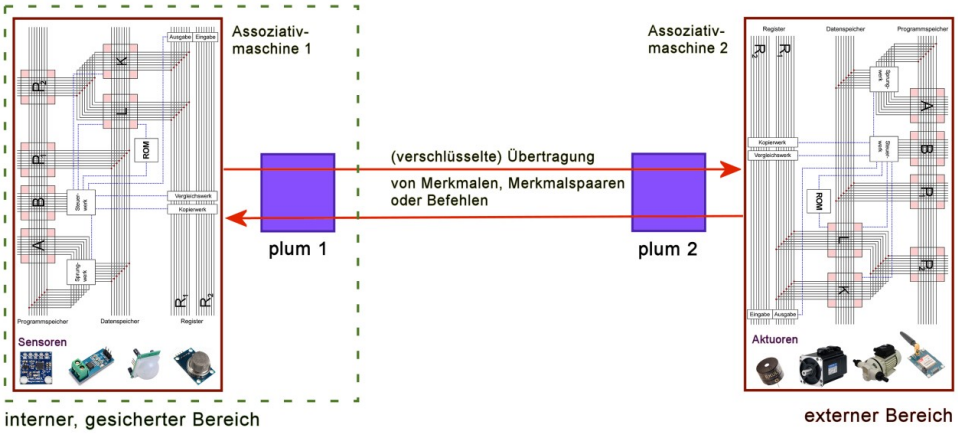
Assoziativmaschine Use Case *IoT*: *Absicherung einer Anlage*

Absicherung einer Anlage mit Assoziativmaschinen



Zwei Assoziativmaschinen sichern eine Anlage zum Messen, Steuern und Regeln ab.

Situation

Eine in einem internen, gesicherten Bereich stehende Anlage liefert über ihre Sensorik Werte, die von einer externen Anlage ausgewertet und in Aktionen umgesetzt werden sollen. Angriffe auf die interne Anlage sind nicht zu erwarten, Angriffe auf die externe Anlage und die Übertragungswege sollen verhindert werden.

Besonderheiten / Neuheiten:

Die Assoziativmaschinen 1 und 2 sind **störunanfällig** und **virenfest**; sie arbeiten ihre Programme auch noch zuverlässig ab, wenn äußere Einflüsse stören (elektromagn. oder ionisierende Strahlung u.a.m.). Die abzuarbeitenen Programme haben trotz gleicher Wirkung bei jedem Neustart wechselnde Darstellungen, also z.B. keine wiederkehrenden Bytesequenzen für ihre Befehlscodes. Daher ist das Einschleusen von Schadsoftware oder ein Mitprotokollieren auszuschließen. Zusätzliche Sicherheit auf den Übertragungswegen schaffen die Verschlüsselungsgeräte plum1 und plum2, deren Wirkung ebenfalls auf Assoziativmatrizen-Technologie beruht.

Dank der innewohnenden **Fehlertoleranz**, d.h. Fähigkeiten zur Mustererkennung, kann die Assoziativmaschine eine sichere Zuordnung von schwankenden Sensordaten zu validen Merkmalen liefern, die in den externen Bereich übertragen werden (oder vor Ort eine Aktion auslösen). Derartiges wurde bereits beim "Lesen" bzw. Zuordnen von Überweisungsträgern, Briefadressen, Datenbankeinträgen, bei Terminologieerkennung, Unterschriftenerkennung, KFZ-Kennzeichenerkennung eingesetzt.

Anstelle mit Sensordaten sei die Fehlertoleranz des assoziative Ansatzes hier mit textuellen Daten illustriert. Die Anfrage war "Kundennummer". Man erkennt fehlerhafte -Kundenummer- sowie ähnliche Kandidaten - Urkundennummer - Kundenstammnummer etc. Bei dieser Erkennung wurde kein zusätzliches Werkzeug verwendet (wie Theasaurus o.ä.).

ENDE Use Case Assoziativmaschine im IoT