

# Inhaltsverzeichnis

## Content

|   |           |
|---|-----------|
| <b>1 Einleitung .....</b>   | <b>1</b>  |
| <b>2 Stand der Technik in Forschung und Industrie .....</b>                                     | <b>7</b>  |
| 2.1 Aufbau cyberphysischer Produktionssysteme .....   | 7         |
| 2.1.1 Beschreibung von Systemkomponenten .....  | 8         |
| 2.1.2 Steuerungskonzepte für CPPS .....   | 12        |
| 2.1.3 Ansätze zur Orchestrierung von Daten .....  | 15        |
| 2.2 Sicherheit von Automatisierungssystemen.....  | 17        |
| 2.2.1 Relevante Normen .....  | 17        |
| 2.2.2 Ausführung von Sicherheitssystemen in der Industrie .....                                 | 23        |
| 2.2.3 Sicherheitsfunktionen .....   | 25        |
| 2.2.4 Ansätze zur inhärent sicheren Konstruktion in CPPS .....                                  | 25        |
| 2.3 Vertragsbasierte Gestaltung von Steuerungsfunktionen .....                                  | 27        |
| 2.4 Fazit .....   | 31        |
| <b>3 Zielsetzung, Aufgabenstellung und Vorgehensweise .....</b>                                 | <b>33</b> |
| 3.1 Aufgabenstellung und Zielsetzung .....  | 33        |
| 3.2 Vorgehensweise der Arbeit .....   | 34        |
| 3.3 Beschreibung des Demonstrationsszenarios .....  | 37        |
| <b>4 Identifikation der sicherheitsrelevanten Anforderungen an CPPS .....</b>                   | <b>41</b> |
| 4.1 Einordnung der Ziele und Herausforderungen von CPPS in den<br>Automatisierungskontext ..... | 42        |
| 4.1.1 Bedeutung von CPPS für die Automatisierungstechnik.....                                   | 43        |
| 4.2 Ableitung der allgemeinen Anforderungen an CPPS.....  | 44        |
| 4.2.1 Anbindung der Produktionsassets.....  | 45        |
| 4.2.2 Extraktion von Wissen durch die Analyse der bereitgestellten<br>Daten.....                | 47        |
| 4.2.3 Rückführung von Wissen in alle Produktionslebenszyklusphasen<br>.....                     | 48        |
| 4.2.4 Zwischenfazit .....   | 49        |
| 4.3 Beschreibung von Sicherheitssystemen.....   | 50        |
| 4.4 Ableitung der Anforderungen an sicherheitsbezogene<br>Systemkomponenten.....                | 54        |
| 4.4.1 Anforderungen an die Infrastruktur.....   | 55        |
| 4.4.2 Anforderungen an die bereitgestellten Funktionen .....                                    | 57        |
| 4.4.3 Zwischenfazit .....   | 60        |

---

|  |            |
|--|------------|
| <b>5 Entwicklung einer inhärent sicheren Systemarchitektur .....</b>   | <b>63</b>  |
| 5.1 Auswahl der Systemkomponenten .....  | 63         |
| 5.1.1 Produktionsbedingte Funktionen .....   | 63         |
| 5.1.2 Konzeption einer cyberphysischen Produktionskomponente für steuerungstechnische, sicherheitsbezogene Systemkomponenten ..... | 66         |
| 5.2 Anordnung der Systemkomponenten .....  | 69         |
| 5.2.1 Konzept zur Datenorchestrierung für die Erstellung dynamischer Digitaler Schatten .....                                      | 69         |
| 5.2.2 Anordnung von Funktionen innerhalb des Cloud und Edge Computings .....   | 75         |
| 5.2.3 Erweiterung des CPPS um sicherheitsbezogene Funktionalitäten .....   | 77         |
| 5.2.4 Zwischenfazit .....  | 80         |
| 5.3 Sicherheitstechnische Betrachtung .....  | 81         |
| 5.4 Fazit .....  | 82         |
| <b>6 Identifikation und Überwachung von Systemgrenzen .....</b>  | <b>85</b>  |
| 6.1 Identifikation von sicherheitsrelevanten Informationen .....   | 85         |
| 6.1.1 Beschreibung von Systemgrenzen im Kontext der Produktion .....   | 87         |
| 6.1.2 Implementierung von Sicherheitsfunktionen .....  | 89         |
| 6.2 Extraktion und Überwachung räumlicher Systemgrenzen .....  | 91         |
| 6.2.1 Festlegung der Zellgrenzen mittels Ebenen .....  | 92         |
| 6.2.2 Simulation der Zellgrenzen mittels PyBullet .....  | 94         |
| 6.2.3 Erkennen von kritischen Zuständen mittels Kamera und Bildverarbeitung .....  | 97         |
| 6.2.4 Zwischenfazit .....  | 102        |
| 6.3 Beschreibung und Ausführung des gewünschten Verhaltens mithilfe von Verträgen .....  | 103        |
| 6.4 Methodik zur Überwachung von Sicherheitsfunktionen .....   | 108        |
| 6.5 Fazit .....  | 110        |
| <b>7 Referenzimplementierung und Evaluierung .....</b>   | <b>111</b> |
| 7.1 Beschreibung der Referenzimplementierung .....   | 111        |
| 7.1.1 Erweiterung der bestehenden Infrastruktur (Redundanz) .....  | 116        |
| 7.1.2 Evaluierung der Erweiterung der Referenzinfrastruktur .....  | 118        |
| 7.1.3 Implementierung der Sicherheitsfunktionen .....  | 122        |
| 7.1.4 Überwachung der Eingänge der Sicherheitsfunktionen .....   | 125        |
| 7.2 Evaluierung der Referenzimplementierung .....  | 126        |
| 7.3 Fazit .....  | 129        |

---

|           |  |            |
|-----------|--|------------|
| <b>8</b>  | <b>Zusammenfassung und Ausblick.....</b>               | <b>131</b> |
| 8.1       | Zusammenfassung.....                                   | 131        |
| 8.2       | Ausblick.....  | 132        |
| <b>9</b>  | <b>Literaturverzeichnis.....</b>                       | <b>137</b> |
| <b>10</b> | <b>Anhang .....</b>                                    | <b>157</b> |
| 10.1      | Tabellen .....   | 157        |
| 10.2      | Ontologien.....  | 163        |
| 10.3      | Integration der sicherheitsbezogenen Komponenten ..... | 165        |
| 10.4      | Detaillierte Beschreibung der Viola-Jones Methode..... | 166        |