1 Einleitung

Durch die fortschreitende digitale Transformation der Produktion unter dem Begriff Industrie 4.0 werden neue Steuerungskonzepte vorangetrieben [VOGE20; KAGE13; ABEL16]. Sie verfolgt das Ziel einer ressourcenschonenden und energieeffizienten, flexiblen Produktion. Diese Entwicklung wird durch das Internet der Dinge und die damit verbundenen eingesetzten Services unterstützt [SCHU16b]. Es werden Konzepte, wie die auftragsgesteuerte Produktion, adaptierbare Fabrik und selbstorganisierende Logistik mithilfe von Multiagentensystemen untersucht, die einen modularen Aufbau der Produktion als Grundlage sehen. Sowohl die Hardware, als auch die Software bzw. Steuerung muss zur Umsetzung der Konzepte flexibel gestaltet werden [VOGE20].

Die Umsetzung solcher flexiblen Produktionssysteme stockt, da zurzeit Defizite durch zu wenige und unstrukturierte Daten aus Produktionsbetrieben vorliegen, Planungssysteme nicht adaptiv sind und zudem Daten im Planungssystem nicht kontinuierlich überprüft werden [SCHU16b]. Außerdem wird befürchtet, dass neue Geschäftsmodelle für Unternehmen nicht profitabel sind und die bisher vorherrschenden Erfolgsmodelle der Unternehmen bedrohen [BREC21a]. Geräte und Maschinen sollen immer häufiger eigenständige Entscheidungen treffen. Dies bedeutet, dass sie auch Fehlentscheidungen treffen können. Im Schadensfall muss geprüft werden, ob das Verhalten der Maschine vorhersehbar und vermeidbar war [GRÜT16]. Dies führt zu weiteren Vorbehalten bezüglich des Einsatzes flexibler Produktions- und Steuerungssysteme [BREC21a].

Da Sicherheit einfach, übersichtlich, nachvollziehbar und überprüfbar sein muss, ist die Umsetzung flexibler Sicherheitslösungen in adaptiven System nicht vorgesehen. Sicherheit wird nicht von vornherein mitgedacht, sondern folgt in der Regel den sich nach und nach durchsetzenden Trends der Flexibilisierung. Nach wie vor werden Sicherheitssysteme konservativ ausgelegt, sodass im Zweifel immer ein elektromechanischer Not-Halt ausgeführt wird. Dies erlaubt wenig Raum für Flexibilität. Sicherheitssteuerungen müssen komplexere Vorgänge abdecken und daher intelligenter und dynamischer werden. Dies beinhaltet auch, die bisher vorhandenen Logik-Funktionen stetig zu erweitern. [PILZ17]

Die Haftungsfrage im Falle eines Schadens geht einher mit der Frage nach Verantwortung. Eine Person oder ein Unternehmen muss mit persönlichen und rechtlichen Konsequenzen rechnen. Rechtliche und technische Rahmenbedingungen, die durch Regeln, Normen und politische Vorgaben definiert sind, müssen eingehalten werden, um der Verantwortung über das technische System gerecht zu werden. Diese Verantwortung umfasst den gesamten Produktlebenszyklus eines technischen Systems und damit die Bereiche der technischen Sicherheit, dem Schutz der Mitarbeitenden am Arbeitsplatz, Umweltverträglichkeit, Ressourceneinsatz/-verbrauch, Leistungsfähigkeit und Funktionsfähigkeit. Es muss daher immer klar sein, wer sich wofür vor wem zu verantworten hat. Neben der Frage, wie lange und aus welchen Gründen jemand verantwortlich ist, spielt jedoch auch das Wissen über mögliche Folgen und der Umgang mit den bestehenden Unsicherheiten eine entscheidende Rolle. [ACAT21]

Um Unternehmen und den auszuführenden Personen einen rechtlichen Rahmen zur Übernahme der Verantwortung zu geben, müssen Maschinen, die auf dem europäischen Markt bereitgestellt werden, grundlegenden Sicherheits- und Gesundheitsschutzanforderungen der Richtlinie 2006/42/EG (Maschinenrichtlinie) erfüllen [DEUT93]. Diese Richtlinie beschreibt das Miteinbeziehen von wichtigen Sicherheitsgrundnormen, wie die ISO 12100, die die Entwickler eines technischen Systems durch ein definiertes Vorgehen zur Abschätzung und Minimierung des Risikos unterstützen. Diese Richtlinie und die sich anschließenden Sicherheitsnormen wurden jedoch für statische, nicht-adaptive Systeme entwickelt, sodass für neue Entwicklungen im Bereich der datenbasierten Produktionsoptimierung und -anpassung bisher wenige Regeln vorliegen.

Aus rechtlicher Perspektive wird erwartet, dass bei einem Schadensfall nach wie vor der Beweis angeführt werden muss, inwiefern ein Fehlverhalten zu erwarten war. Die zugrundeliegenden Daten in ihrer Masse und letztendlich die für die Fehlentscheidung relevanten Daten können nicht einfach zur Beweisführung herangezogen werden. Hinzu kommt, dass die deliktische Haftung abhängig von der Berechenbarkeit, also einer konkreten Berechnungsanweisung des Systems, ist [GRÜT16]. Daher wird davon ausgegangen, dass zukünftig keine konkreten Handlungen in autonomen Systemen mehr vordefiniert und abgesichert werden, sondern das System einer Überwachung unterzogen wird. Zur Bewertung des Sorgfaltsmaßstabs werden vorerst Einzelfälle betrachtet. Hierbei werden die Auswahl (geeignet für Einsatzzweck), Bedienung (ordnungsgemäße Dokumentation) und Überwachung (System genügt während des Einsatzes den Sicherheitsanforderungen) beurteilt. Der Aufwand zur Protokollierung wird umfangreicher. Durch die Flexibilisierung von Produktionsanlagen und einen damit verbundenen erhöhten Automatisierungsgrad verschiebt sich das Sorgfaltsmaß vom Nutzer zum Hersteller. Die Festlegung des Einsatzgebietes und die damit verbundene Überwachung des Systems gewinnen im Vergleich zu Bedienfehlern an Wichtigkeit. [HORN16]

Die Frage der Rechtssicherheit bei Verwendung von Algorithmen der künstlichen Intelligenz (KI) besteht im allgemeinen schön länger. Hierbei stellt sich die Frage, ob der Mensch zur Verantwortung gezogen werden kann, wenn der Algorithmus eine falsche Entscheidung trifft. Es besteht die Annahme, dass der Programmierer immer das Verhalten der Maschine im Detail beherrscht und erklären kann, wie die verwendeten Algorithmen funktionieren. Ein Fehler im System ist damit immer ein Fehler des Programmierers. Durch die Nutzung von KI wechselt der Programmierer seine Rolle zum Schöpfer. Es entsteht also eine Verantwortungslücke [MATT04]. Zur Gewährleistung der Sicherheit muss sichergestellt werden, dass alle potenziellen Risiken aufgrund von Systemfehlern entweder ausgeschaltet oder in akzeptabler Weise gemindert werden. Daher müssen alle Fehler, die zu einer Gefährdung der Herstellungsprozesse führen könnten, im Rahmen der Sicherheitsgewährleistung vor dem Einsatz analysiert und kontrolliert und in der Betriebsphase überwacht und kontrolliert werden [JARA18].

Zentrale Faktoren zur Rechtssicherheit sind die Verfügbarkeit und der Zugang, die Integrität, die Vertraulichkeit und die Verwertung der Daten. Durch die flexible Kommunikation zwischen Anlagen und Komponenten können im Verbund arbeitende cyberphysische Produktionssysteme (CPPS) Fehler und somit Sach- und Vermögensschäden verursachen. Hier wird insbesondere auf die Verschuldungshaftung und der damit verbundene Sorgfaltsmaßstab bei der Entwicklung solcher Systeme hingewiesen [HORN17]. Die Festlegung der Grenzen des Einsatzgebiets und die Überwachung des Systems spielen daher eine zentrale Rolle [HORN16]. Die Risikobeurteilung sollte also nicht erst am Ende der Entwicklung eines flexiblen, adaptiven Produktionssystems durchgeführt werden, sondern frühzeitig integriert und iterativ bei der Entwicklung mitgedacht werden [SCHU18; PILZ17].

Auf Basis dessen ist das Ziel dieser Arbeit, sich mit dem Aufbau von CPPS auseinanderzusetzen und Konzepte für sichere CPPS zu entwickeln. Neben dem Aufbau einer sicheren Infrastruktur, werden Mechanismen zur eindeutigen Bereitstellung von Daten vorgestellt, mit denen dynamische Sicherheitsfunktionen, die zum einen das Verhalten, aber auch die Systemumgebung überwachen. Diese Funktionen werden implementiert und evaluiert.

Der Stand der Technik in Forschung und Industrie (vgl. Kapitel 2) fasst die wesentlichen Eigenschaften von CPPS und Entwicklungen im Bereich der Sicherheit zusammen und gibt Aufschluss über vorhandene Forschungslücken. Zum Schließen der identifizierten Forschungslücken wird in Kapitel 3 die Zielsetzung und die Vorgehensweise abgeleitet, sowie das Demonstrationsszenario vorgestellt. Im ersten Schritt werden dazu in Kapitel 4 Anforderungen an CPPS und an die Sicherheit steuerungs-technischer Systeme identifiziert. Auf Basis der Anforderungen wird in Kapitel 5 eine inhärent sichere Systemarchitektur bezogen auf die eindeutige Bereitstellung von Daten aus heterogenen Datenquellen, die Anordnung von Funktionen im System und eine sichere Kommunikationsinfrastruktur vorgestellt und unter Berücksichtigung von Anforderungen aus der Sicherheit untersucht. Anschließend werden gemäß dem Vorgehen zur Risikominimierung beispielhaft Systemgrenzen identifiziert und in flexible Sicherheitsfunktionen überführt (vgl. Kapitel 6). Die Systemarchitektur wird abschließend gemeinsam mit den Sicherheitsfunktionen implementiert und evaluiert (vgl. Kapitel 7).