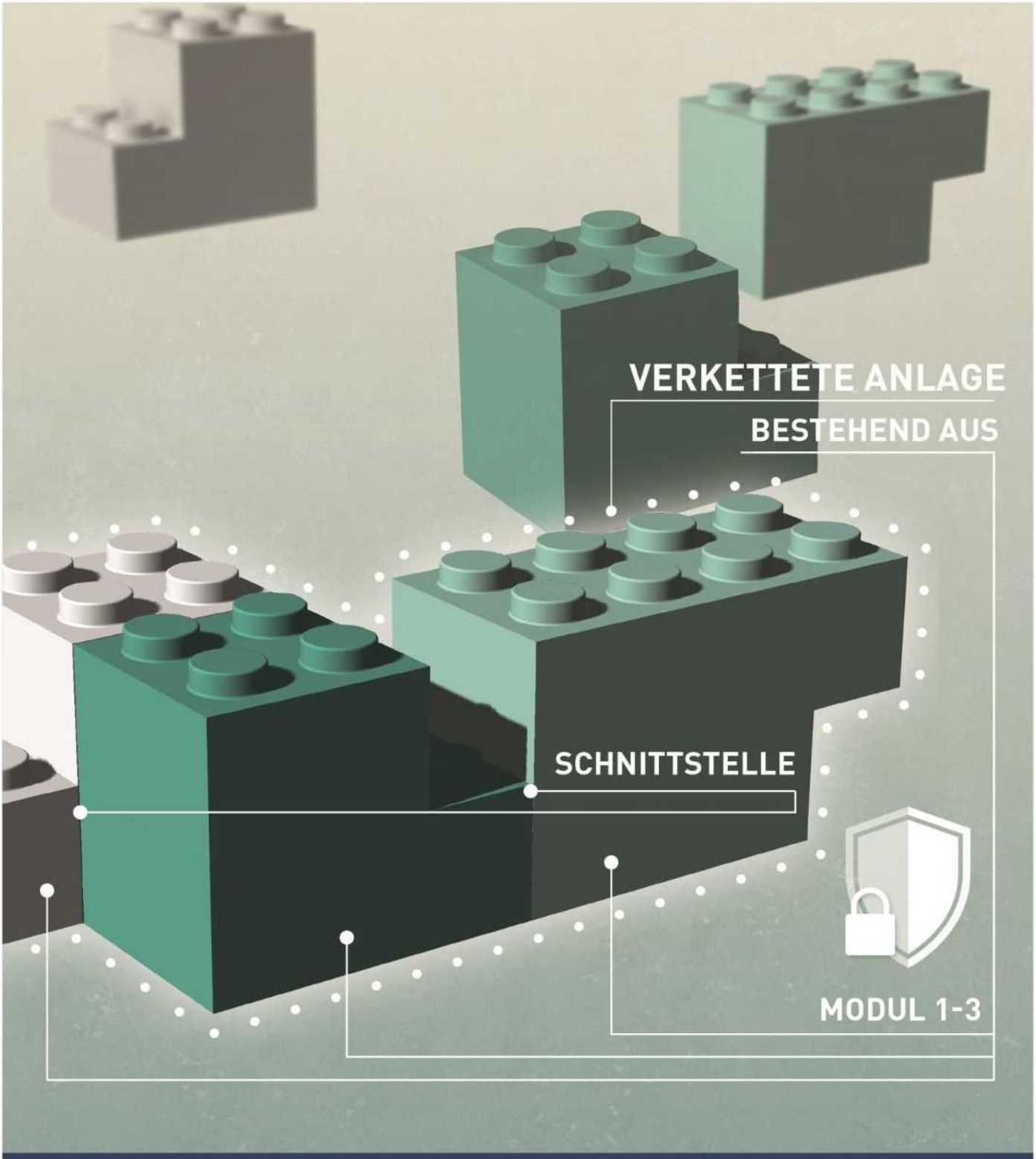

Smart Safety - Sicherheit in modularen Produktionsprozessen

Whitepaper SF-3.2: 04/2019

smartFactory KL®

SmartFactory^{KL} Whitepaper SF-3.2: 04/2019

Smart Safety - Sicherheit in modularen Produktionsprozessen

Abstract

Die Arbeitsgruppe 1 „Smarte Infrastruktur“ der ***SmartFactory***^{KL} befasst sich mit dem Thema Safety in modularen Industrie 4.0-Produktionsanlagen.

Auch heute ist das Grundprinzip der funktionalen Sicherheit die Risikominderung und nicht der sichere Ausschluss aller möglichen Risiken. Dieses Konzept wird durch den Einsatz von Agentensystemen nicht verletzt. Vielmehr besteht die Möglichkeit, unerkannte Risiken zu entdecken und entsprechende Maßnahmen einzuleiten.

Anhand der Beschreibung von sicheren Profilen, welche innerhalb der Verwaltungsschale (vgl. DIN SPEC 91345) definiert und abgelegt werden, konnte diesbezüglich ein Teilkonzept entwickelt werden, welches die modulare Zertifizierung von Maschinengruppen ermöglichen soll. Aufbauend auf diesen Überlegungen wurde das bestehende Konzept fortentwickelt.

Keywords

Safety, Industrie 4.0, automatische Zertifizierung

Autoren

Hagen Burchardt	Bosch Rexroth AG
Marco Sprenger	B&R
Steffen Horn	Phoenix Contact Electronics GmbH
Joachim Merx	Pilz GmbH & Co. KG
Simon Schönhar	Pilz GmbH & Co. KG
Marius Blügel	Technologie-Initiative SmartFactory KL e.V.
Tobias Thielen	Technologie-Initiative SmartFactory KL e.V.
Dr. Detlev Richter	TÜV SÜD Product Service GmbH
Werner Varro	TÜV SÜD Product Service GmbH
Enrico Seidel	TÜV SÜD Product Service GmbH
Michael Pfeifer	TÜV SÜD Industrie Service GmbH
Pascal Staub-Lang	TÜV SÜD Industrie Service GmbH

Inhaltsverzeichnis

1. Zielsetzung des Whitepapers

Dieses Whitepaper fasst die aktuellen Ergebnisse der Arbeitsgruppe zum Thema Safety an modularen Maschinen zusammen. In Zusammenarbeit mit den beteiligten Partnern Bosch Rexroth, B&R, Festo, Phoenix Contact, Pilz und TÜV Süd wurde ein Konzept zur vereinfachten, teil- oder vollautomatisierten Zertifizierung entwickelt und bereits zur Hannover Messe 2018 veröffentlicht [Link zum Whitepaper 2018]. Anhand der Beschreibung von sicheren Profilen, welche innerhalb der Verwaltungsschale (vgl. DIN SPEC 91345) definiert und abgelegt werden, konnte diesbezüglich ein Teilkonzept entwickelt werden, welches die modulare Zertifizierung von Maschinengruppen ermöglichen soll. Aufbauend auf diesen Überlegungen wurde das bestehende Konzept um mehrere Ebenen der sicherheitstechnischen Überprüfung von modularen Maschinen erweitert. Dabei soll gezeigt werden, wie durch die Definition und Nutzung von anwendungsfallunabhängiger, zertifizierter Software die Schnittstellenkomplexität von verketteten Anlagen auf ein beherrschbares Niveau reduziert werden kann.

2. Motivation

Mit Verweis auf die umfassenden Ausführungen innerhalb des Whitepapers HM18 soll einleitend die Notwendigkeit einer neuen Betrachtungsweise von Maschinensicherheit im Zeitalter von Industrie 4.0 erläutert werden. Die *SmartFactory*^{KL} zeigt nun seit mehreren Jahren durch Forschung und Anwendung, wie die Digitalisierung von Prozessen die Produktion und die Gesellschaft im Allgemeinen nachhaltig verändern wird und es auch heute schon tut. In diesem Zusammenhang wurden unter anderem die Themen „Modularität“ und „Flexibilität“ durch die Anwendungsszenarien „Plug’n’Produce“ und „Fertigung Losgröße 1“ veranschaulicht und Ihre Notwendigkeit für eine konkurrenzfähige Wirtschaft nachgewiesen. Allein durch die Betrachtung dieser beiden Anwendungsszenarien wird deutlich, dass es durch die Digitalisierung der Produktion im Sinne von cyberphysischen Produktionssystemen (kurz: CPPS) zu einer kaum beherrschbaren Komplexitätssteigerung in der Anwendung kommt. Dabei ist bereits heute ein Zielkonflikt zwischen der Automatisierungstechnik und der Sicherheitstechnik entstanden. Das Ziel der modernen Automatisierungstechnik ist keineswegs auf die Mechanisierung und autonome Steuerung von statischen Prozessen beschränkt, sondern ist vielmehr darin begründet, flexibel auf veränderliche Anforderungen zu reagieren und damit möglichst dynamische Prozesse abbilden zu können. Dementgegen steht das Ziel der Sicherheitstechnik, den Betreiber und Bediener der Produktionsmittel zu schützen, indem definierte Prozesse analysiert und durch statische Lösungen abgesichert werden.

Die Arbeitsgruppe Safety der *SmartFactory*^{KL} versteht es als eigene Aufgabe, diesen Zielkonflikt zu analysieren und Möglichkeiten zu finden den Menschen bei der Bewertung komplexer sicherheitsrelevanter Zusammenhänge mittels aktueller Technologien und vorgegebener Semantik in ausreichendem Maße zu unterstützen. Damit wird der Rahmen für den sicheren, flächendeckenden Einsatz von adaptiven Automatisierungslösungen innerhalb dynamischer Prozesse gesetzt.

Unter dem Oberbegriff „Smart Safety Automation" soll innerhalb dieses Dokumentes ein Zielsystem aufgestellt werden, welches den Konflikt zwischen klassischer Sicherheitstechnik und moderner Automatisierungstechnik aufzeigt. Anschließend wird darauf aufbauend das Konzept der Arbeitsgruppe Safety als Lösungsansatz für diesen Zielkonflikt vorgestellt. Dabei wird explizit auf die Notwendigkeit eines einheitlichen Safety-Protokolls und einer einheitlichen Semantik eingegangen. Zur Veranschaulichung des Konzeptes folgt die Beschreibung von „Smart Safety Automation" anhand einer Realisierung innerhalb der *SmartFactory*^{KL}.

3. Theorie

3.1 Systemtheoretische Betrachtung von Industrie 4.0 Anlagen

Industrie 4.0 Anlagen erfüllen schon heute die Eigenschaften komplexer Systeme. Sie sind Agentenbasiert[1], nichtlinear, zeigen Emergenzen und globale Interaktionen, sind offen bezüglich Stofftransporte, haben die Möglichkeit zur Selbstregulation und zeigen Pfadabhängigkeiten [vgl. WIKI19]. Anhand der *SmartFactory*^{KL} lässt sich die Einordnung von Industrie 4.0 Anlagen wie folgt erklären: Obwohl die Module selbst in ihrer Komplexität beherrschbar sind und vollumfänglich beschrieben werden können, ergeben sich durch den gemeinsamen Betrieb komplexe Wechselwirkungen zwischen den einzelnen Modulen und ein nichtlineares Störungsverhalten. Wird das momentan eingesetzte fahrerlose Transportsystem in die Betrachtung einbezogen, kann sogar von einem komplexen adaptiven Agentensystem[2] gesprochen werden [STÜTT02]. Aus sicherheitstechnischer Sicht ergeben sich damit Systeme von Systemen, welche sich zur Laufzeit durch eine hohe Dynamik und Flexibilität auszeichnen. Die dadurch entstehenden Unsicherheiten im Systemverhalten stehen im direkten Widerspruch zur klassischen Sicherheitsnachweisführung, die auf der Annahme eines deterministischen, vorhersagbaren Systemverhaltens beruht [LIGG17]. Es

1 Definition Agent nach VDI/VDE 2653 Blatt 1: „abgrenzbare (Hardware- und/oder Software-) Einheit mit definierten →Zielen, die sich auf die Steuerung (gegebenenfalls eines Teils) eines technischen Systems beziehen"

2 Definition Agentensystem nach VDI/VDE 2653 Blatt 1: „Menge von →Agenten, die interagieren, um gemeinsam eine oder mehrere Aufgaben zu erfüllen"

zeigt sich also, dass eine Konformitätsbeurteilung einer komplexen Industrie 4.0 Anlage zum Zeitpunkt der Auslieferung an den Betreiber nur für Teilsysteme möglich ist.

3.2 Status Quo Industrie

Im Safety-Whitepaper 3.1 [SF18] wurde bereits ausführlich der Status-Quo der Industrie beschreiben und auf die Schwierigkeiten im Zusammenhang von häufigen Anlagenänderungen unter Berücksichtigung der Vorgaben der Maschinenrichtlinie hingewiesen.

Zur Erinnerung: In der Praxis muss bei der Änderung der Konfiguration einer Maschinengruppe eine sicherheitstechnische Bewertung erfolgen. Um bereits heute die Modularität einer Anlage, beispielsweise für Serienmaschinen, zu ermöglichen, werden alle möglichen Varianten/Konfigurationen betrachtet, bewertet und validiert. Dies setzt voraus, dass alle Module deren sicherheitstechnischen Eigenschaften bekannt sind und das Vorgehen, wie auch die Ergebnisse, durch einen Verantwortlichen dokumentiert und validiert werden. Dieses Vorgehen ist für modulare I4.0 Anlagen nur bedingt zielführend. Durch die sich ständig ändernden Technologien und die Forderung nach Losgröße 1, kann vorab nicht abgeschätzt werden, welche Anlagenkonfigurationen in der Zukunft benötigt werden.

3.3 Einsatz von Agentensystemen in der Produktion, insbesondere Safety

Um die heute vorherrschenden Probleme bei der sicherheitstechnischen Betrachtung von wandelbaren Systemen zu überwinden, könnten Agentensysteme eingesetzt werden. Dabei bieten diese Methoden durch ihre Fähigkeit aus unbekannten Daten zu lernen die Möglichkeit, dass sich Maschinen flexibel an ihre Kooperationspartner anpassen, um gemeinsam Prozesse durchzuführen.

Der Einsatz von Agentensystemen in der Automatisierungstechnik ist keineswegs neu. Beispielweise wurden in VDI/VDE 2653 Blatt 3 bereits zwölf verschiedene Einsatzszenarien für Agentensysteme in der Automatisierungstechnik vorgestellt. Explizit wird dabei auf den Einsatz in modularen Produktionsanlagen verwiesen. In der *SmartFactory*^{KL} besitzt jedes Produktionsmodul eine dedizierte Steuerung mit dem Ziel, den definierten Produktionsschritt mit den vom Produkt kommunizierten Parametern durchzuführen. Der Einsatz von solchen Agentensystemen ist in den in Kapitel 2 und [Whitepaper HM18] beschriebenen, gewachsenen Anforderungen begründet. Agentensysteme haben dabei den Vorteil, dass durch die konzeptionelle Aufteilung von Zielen, Funktionalitäten und Entscheidungsprozessen auf autonome Einheiten, eine systematische und einfache Dekomposition der Komplexität bei der Entwicklung von verteilten Automatisierungssystemen ermöglicht wird. Dadurch, dass das Wissen über die Problemstellung mittels Ziele in die Agenten integriert wird, wird der Ort der Entscheidung an die Stelle verschoben, an der die meisten Informationen über die Problemstellung vorliegen. Da diese Informationen durch die Interaktion von verschiedenen Agenten unter Umständen erst entstehen, kann ein hohes Maß an Flexibilität und Selbstanpassungsfähigkeit eines technischen Systems im Betrieb erreicht werden. Bei einer agentenorientieren Entwicklung müssen nicht alle möglichen Abläufe bereits beim Entwurf

des Systems bekannt sein. Wesentliche Eigenschaften des Gesamtverhaltens werden erst zur Laufzeit in das Agentensystem aufgenommen [VDI/VDE 2653 Blatt1].

Dem Einsatz solcher Methoden im Bereich der Maschinensicherheit stehen jedoch Vorbehalte gegenüber, z.B. von normativer Seite. Als Beispiel kann der branchenübergreifende Standard IEC 61508 zum Thema Sicherheit elektrisch bzw. elektronisch programmierbarer, sicherheitsbezogener Systeme genannt werden. In Teil 7 sind Methoden der künstlichen Intelligenz oder auch dynamische Rekonfiguration für SIL 2 bis 4 als „ausdrücklich nicht empfohlen“ deklariert. Bei einem erstmaligen Einsatz eines bestimmten Agentensystems in der Safety ist somit ab Beginn der Sicherheitsplanung eine fundierte Nachweisführung sowie ausgiebige Validierung notwendig.

Das Spannungsfeld zwischen Safety und Industrie 4.0 beschränkt sich jedoch keineswegs auf den Einsatz intelligenter Methoden oder die IEC 61508. Auch bisherige Arbeitsweisen zur Erfüllung von Vorgaben der Maschinenrichtlinie 2006/42/EG sind zu hinterfragen. So kann bei häufig wechselnden Anlagenkonfigurationen einer Produktionslinie das Ausdrucken, Unterschreiben und manuelle Archivieren der Konformitätserklärungen einen nicht mehr vernachlässigbaren zeitlichen Aufwand einnehmen und erscheint im Zeitalter der Industrie 4.0, digitalen Signaturen oder auch sicheren Online-Identifikationsverfahren als nicht mehr zeitgemäß - zumal die Maschinenrichtlinie eine Konformitätserklärung nicht explizit in Papierform fordert, sondern lediglich das Vorliegen des unterzeichneten Originals.

Ziel der folgenden Ausführungen ist es daher, einen Safety-Ansatz für flexible, modulare Industrie 4.0 Anlagen aufzuzeigen. Dabei wird bewusst auf eine strikte und formale Interpretation der existierenden Normen verzichtet und versucht, die zugrunde liegende Intention der bestehenden Normen durch den Einsatz von intelligenten Systemen vor dem Hintergrund der beschriebenen gestiegenen Anforderungen umzusetzen.

4 Smart Safety - Sicherheit in modularen Produktionsprozessen

Der folgende Ansatz lässt sich in drei Teilbereiche gliedern. Zunächst soll die Umsetzung der Basis-Risikobeurteilung (vgl. Whitepaper HM 2018) eines einzelnen Industrie 4.0-Moduls innerhalb der *SmartFactory*^{KL} anhand von Entscheidungsbäumen erläutert werden. Anschließend wird auf den Einsatz von Risiko-Reduzierungs-Agenten an den Modulschnittstellen eingegangen, welche ebenfalls anhand von definierten Entscheidungsbäumen die Schnittstellen der verketten Anlage sicherheitstechnisch validieren soll. Abschließend wird auf die die verschiedenen Datenquellen eingegangen, welche zur übergreifenden Safety-Validierung notwendig sind.

Folgendes Schaubild beschreibt dieses Vorgehen graphisch:

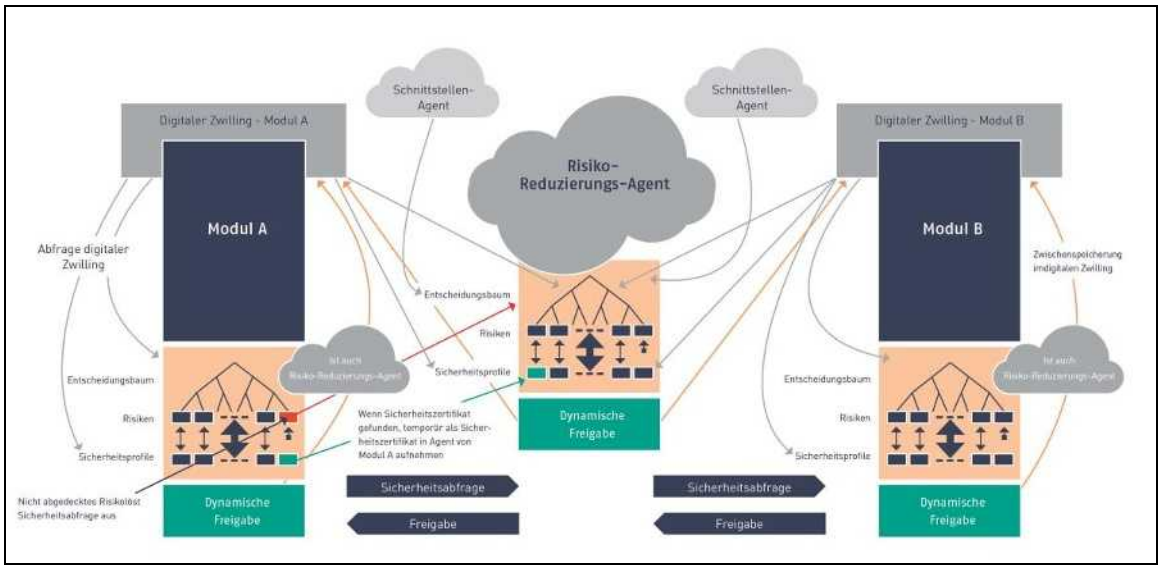

Abbildung 1: Smart Safety Risiko-Reduzierungs-Agentensystem

4.1 Umsetzung einer dynamischen Freigabe eines einzelnen Moduls

Wie bereits eingangs erwähnt, wird das ursprünglich alleinige Ziel der Safety, den Schutz des Menschen zu gewährleisten, immer mehr durch ein komplexes Zielsystem ersetzt. Dabei werden Ziele wie „maximale Verfügbarkeit“ oder „Systemgrenzen nicht verlassen“ zu dem Primärziel „Personen nie verletzen“ in die Überlegungen mit einbezogen. Da diese Ziele oft im Widerspruch zu dem Primärziel der Safety stehen, wird eine dynamische Betrachtungsweise zwingend erforderlich, um das Zielsystem optimieren zu können. Eine Möglichkeit, die Dynamik von modularen Produktionsanlagen beherrschbar zu machen, besteht in der Realisierung von auf Entscheidungsbäumen basierenden intelligenter Basis-Risikobeurteilungen von Modulen zur Laufzeit.

Hierbei wird für jedes Modul ein Entscheidungsbaum benötigt, welcher alle möglichen Safety-Zustände anhand vordefinierter Parameterräume enthält. Diese Parameterräume müssen vom Hersteller bereits in der Entwicklungsphase definiert werden und müssen manipulationssicher abgelegt sein. Ein Betrieb des Modules außerhalb der definierten Parameterräume führt zum sofortigen Entzug der Freigabe und damit zum Stillstand des Maschinenmoduls. Da die Verbindung von allen prozessrelevanten Parameterräumen in einem Entscheidungsbaum schnell zu einer hohen Unübersichtlichkeit führt, ist es notwendig, eine Expertensoftware zur Entwicklung dieser Entscheidungsbäume bereit zu stellen. Dabei muss das Wissen von Safety-Experten über die notwendigen Abfragen zur Identifikation von Risikopotentialen erfasst und automatisiert den durch die Parameterraumdefinitionen aufgespannten Pfade hinzugefügt werden. Die Blätter (= Enden eines Entscheidungsbaumes) des Entscheidungsbaumes entsprechen den möglichen Risiken bei den jeweiligen Prozessparametern. Endet ein Pfad in einem Blatt mit einem nicht tolerierbaren

Restrisiko, müssen die vorhandenen Sicherheitsprofile (vgl. Whitepaper HM18) abgefragt werden und dem Risiko mit Hilfe von Risiko-Reduzierungsagenten gegenübergestellt werden. Entsprechen die innerhalb der Sicherheitsprofile abgelegten Sicherheitseinrichtungen dem durch das Restrisiko geforderte Safety Integrity-Level, kann eine Freigabe zur Laufzeit erstellt werden. Ist die Sicherheitseinrichtung nicht ausreichend oder steht einem Risiko kein Sicherheitsprofil entgegen, so wird die Freigabe für die eingestellten Parameter entzogen. Entsprechend des Whitepapers zur HM18 werden die erstellten aber auch entzogenen Freigaben sicher abgelegt und stehen somit zukünftig zur Verfügung. Die hier genannten Entscheidungsbäume können vollständig vom Hersteller definiert und dem Betreiber mitgeliefert werden. Dadurch wird es dem Betreiber ermöglicht, eine Losgrößen 1 Fertigung bei im Vorfeld unbekannten Prozessen zu realisieren, ohne die Vorgaben des Arbeitsschutzgesetzes zu verletzen. Die Expertensoftware zum Zugriff auf die Entscheidungsbäume muss dabei so gestaltet sein, dass bei nicht erfolgreicher automatischer Risikobewertung eine manuelle sowie autorisierte Nachbewertung durch einen Safety-Experten möglich ist.

4.2 Einsatz von Risiko-Reduzierungsagenten an den Modulschnittstellen

Die Schnittstelle zwischen den Produktionsmodulen unterliegt anderen Bedingungen. Hierbei ist es notwendig, für verschiedene Branchen Standardentscheidungsbäume zu entwickeln, die sich den Entscheidungsbäumen der Module selbst bedienen. Dabei werden nicht die Parametereinstellungen der einzelnen Maschinenmodule, sondern lediglich die ermittelten Risiken an den Schnittstellen zwischen den Modulen betrachtet. Diese Risiken entsprechen in der Regel den Blättern in den Entscheidungsbäumen der Einzelmodule, welchen kein Sicherheitsprofil des entsprechenden Moduls entgegensteht. Diese Problematik ergibt sich aus den aus Sicht des Modulherstellers unbekannten Umweltbedingungen im Einsatz. Anstatt der Definition eines bestimmungsgemäßen Gebrauchs, wird also versucht, die Feststellung des sicheren Anlagenverbundes durch die Kombination der dynamischen Freigaben der Einzelmodule und der dynamischen Schnittstellenbewertung zu ermöglichen. Aufgrund der unbekannten Umgebung wird vorgeschlagen, zustandsabhängige Risiken in den Modulen wie auch an den Schnittstellen zwischen den Modulen durch zusätzliche Schnittstellen-Risiko-Reduzierungsagenten zu bewerten. Diese werden durch den Maschinenhersteller definiert und können die Notwendigkeit der Existenz eines Sicherheitsprofils für bestimmte Zustände aufheben (vgl. Kapitel 5).

4.3 Datenquellen und Semantik der Risiko-Reduzierungsagenten

Um die notwendigen Daten zur Validierung zu erhalten, werden mehrere Datenquellen benötigt. Zunächst muss jedes CPPS in seiner Verwaltungsschale einen digitalen Zwilling[3] zur Vorhaltung der Prozess- und Safetydaten besitzen. Damit werden die vom Hersteller definierten Parameter-

[3] Erläuterung zum Verständnis des digitalen Zwillings: dieser das digitale Abbild der Maschine mit Kinematik-Beschreibung/ Funktionen. Die Verwaltungsschale beinhaltet somit den digitalen Zwilling sowie weitere zusätzliche Informationen wie bspw. nach Maschinenrichtlinie geforderte Unterlagen.

räume, wie auch die Sicherheitsprofile bereitgestellt. Zusätzlich müssen die Risiko-Reduzierungs-Agenten zur dynamischen Freigabe bereits in der Entwicklungsphase vom Hersteller definiert werden. Dabei werden alle möglichen Risiken mit ihrem SI-Level definiert und in den Entscheidungsbaum eingebunden. Um die Kommunikation der verschiedenen Risiko-Reduzierungsagenten zu ermöglichen, müssen sowohl die möglichen Risiken, wie auch die Sicherheitsprofile semantisch definiert sein. Dazu ist eine herstellerunabhängige Semantik zu erstellen, auf die der Hersteller an den Blättern des Entscheidungsbaumes zurückgreifen kann. Die in Kapitel 4.2 beschrieben Schnittstellenagenten dienen als zusätzliche Datenbasis für die in der Entwicklung unbekannte Interaktion mit der Umwelt. Die Ausgaben dieser Schnittstellen-Risiko-Reduzierungsagenten können denjenigen Risiken gegenübergestellt werden, welche kein gültiges Sicherheitsprofil innerhalb der Module selbst besitzen.

5 Use-Case SmartFactory^{KL}

Um das Konzept der Smart Safety innerhalb der *SmartFactory*^{KL} zu veranschaulichen, wird dieses im Folgenden anhand eines Use-Cases beschrieben.

5.1 Beschreibung des Use-Case innerhalb der SmartFactory^{KL}

Wie bereits in den Ausführungen zur HM18 beschrieben, nutzt die *SmartFactory*^{KL} für den Werkstücktransport zwischen den verschiedenen Produktionslinien das fahrerlose Transportsystem (FTS) „Robotino“. Innerhalb dieses Use-Cases wird die Interaktion dieses Transportsystems mit der Andockstation und die Interaktion zwischen Andockstation und einem angrenzenden Produktionsmodul, dem „Federmodul“, beschrieben. Alle Akteure werden als eigensichere Module im Sinne des Whitepapers zur Hannover Messe 2018 angesehen. Wie bereits auf der Messe 2018 gezeigt, wird das FTS dynamisch dem Nothaltkreis derjenigen Linie zugeordnet, in deren unmittelbaren Umgebung es sich befindet. Darauf aufbauend, soll innerhalb dieses Use-Cases beschrieben werden, wie die sicherheitstechnische Überprüfung der Interaktion zwischen FTS und Andockstation mithilfe des in Kapitel 4 beschriebenen Konzeptes durchgeführt werden kann.

5.2 Dynamische Freigabe des Federmoduls

Zur Vereinfachung werden innerhalb des Federmoduls folgende Parameterräume definiert:

- „Geschwindigkeit Axialroboter“
    - 0-4 m/s
- „Geschwindigkeit Transportband“
    - 0-2 m/s
- „Zustand Schleuse“
    - „offen“ vs. „geschlossen“

- „Zustand Schutztür“
    - „geschlossen“ vs. „offen“
- „Zustand Zuhaltung Schutztür“
    - „aktiv“ vs. „inaktiv“

Diese Parameterräume sind in dem digitalen Zwilling „Federmodul“ gespeichert und werden eventbasiert in Echtzeit aktualisiert. Sie dienen als Datenbasis für den Risiko-Reduzierungs-Agenten „Federmodul“. Der innerhalb des Agenten ausgeführte Entscheidungsbaum würde in diesem Fall folgendermaßen aussehen:

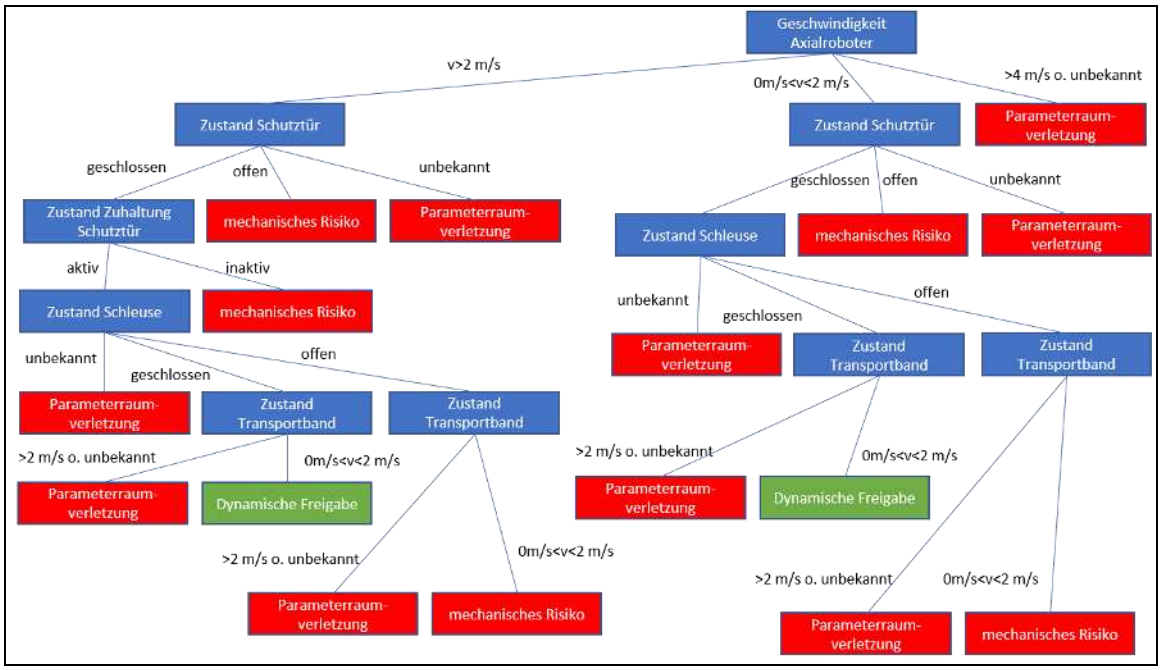

Abbildung 2: Entscheidungsbaum Federmodul

Wie in dem Entscheidungsbaum zu sehen ist, gibt es lediglich zwei Parameterkonfigurationen, in denen das Modul sicher betrieben werden kann. Jede Parameterraumverletzung führt, wie bereits in Kapitel 4 beschrieben, zu einem sofortigen Scheitern der dynamischen Freigabe. Endet der Entscheidungsbaum jedoch in einem Risiko, welches in der Interaktion mit der Umwelt begründet ist, so besteht die Möglichkeit, dieses Risiko mithilfe eines dynamischen Schnittstellenzertifikates aufzuheben.

5.3 Dynamische Freigabe der Andockstation

Die verwendete Andockstation besitzt zwei gegenläufige Transportbänder, um das Werkstück auf einem Werkstückträger von dem angrenzenden Modul bis zum Ende der Produktionslinie oder vom Ende der Produktionslinie bis ins angrenzende Modul zu befördern. Die Bänder können den Werkstückträger jeweils nur in eine Richtung bewegen. Am Ende jedes Transportbandes befindet

sich Sensorik zur Detektion eines Werkstückträgers. Zur Vereinfachung werden innerhalb des Federmoduls folgende Parameterräume definiert:

- „Geschwindigkeit Transportband“
  - 0-2 m/s
- „Werkstück detektiert Ausgang“
  - „Ja“ vs. „Nein“
- „Werkstück detektiert Eingang“
  - „Ja“ vs. „Nein“

Der innerhalb des Agenten ausgeführte Entscheidungsbaum würde in diesem Fall folgendermaßen aussehen:

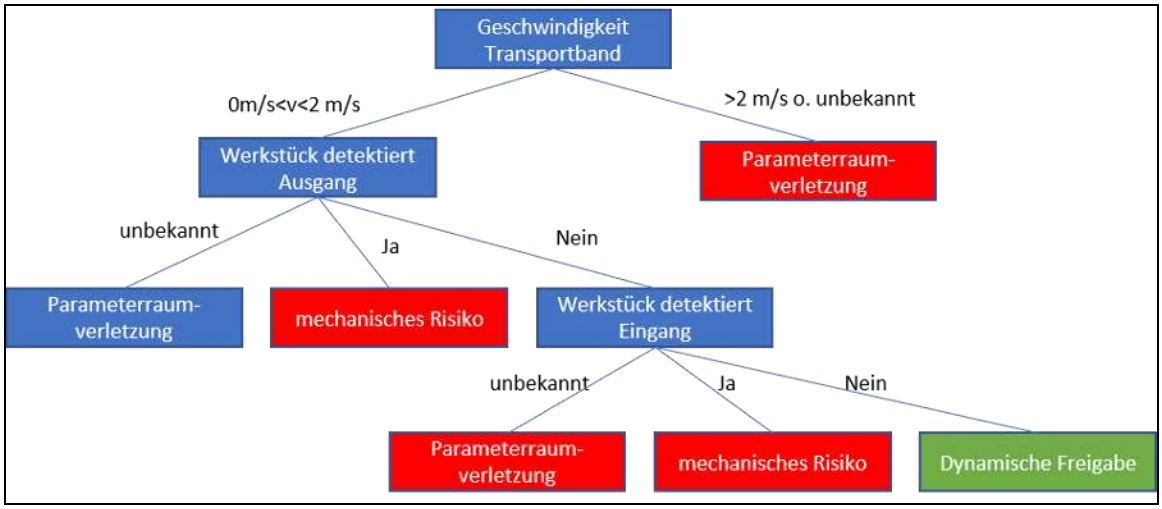

Abbildung 3: Entscheidungsbaum Andockstation

Im Fall dieser Andockstation zeigt sich, dass der Betrieb des Moduls - in Form der Bewegung der Transportbänder – nur erlaubt ist, wenn kein Werkstückträger auf den Bändern detektiert ist. Da ein Single-Betrieb der Andockstation aufgrund Ihres Betriebszwecks nicht möglich ist, sind alle vorhandenen Risiken Schnittstellenrisiken.

5.4 Dynamische Freigabe des fahrerlosen Transportsystems

Da der Betrieb des FTS grundsätzlich auf die Interaktion mit dem Menschen ausgelegt ist und somit sicherheitstechnisch unbedenklich ist, wird nur der prozessrelevante Aufbau des FTS betrachtet. Dieser besteht ebenfalls aus zwei gegenläufigen Transportbändern. Ein Transportband ist für die Aufnahme des Werkstückträgers ausgelegt. Am Ende des Aufbaus wird der Werkstückträger auf das gegenläufige Transportband umgelenkt und am Ende des Bandes von Sensoren detektiert. Die Parameter vereinfachen sich dadurch im Gegensatz zur Andockstation folgendermaßen:

- „Geschwindigkeit Transportband“
    - 0-2 m/s
- „Werkstück detektiert Ausgang“
    - „Ja“ vs. „Nein“

Damit würde der Entscheidungsbaum folgendermaßen aussehen:

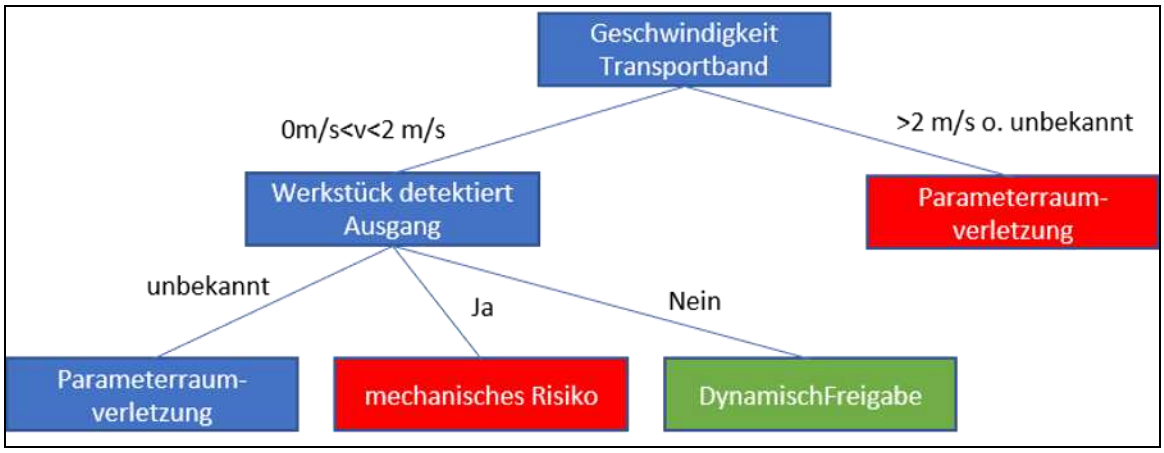

Abbildung 4: Entscheidungsbaum FTS

Entsprechend der Erkenntnisse bei der Analyse des Entscheidungsbaumes der Andockstation ist ein freigegebener Betrieb der Transportbänder des FTS nur möglich, wenn dieser kein Werkstück transportiert. Ein Transport des Werkstücks durch die Transportbänder ist demnach nur nach der Überprüfung der Umweltbedingungen möglich.

5.5 Dynamische Schnittstellenfreigabe

Für das „Federmodul“ ergeben sich anhand des Entscheidungsbaumes 5 Szenarien, welche durch Risiko-Reduzierungs-Agenten überprüft werden können. Diese sind:

- Betrieb mit offener Schutztür mit Robotergeschwindigkeit <2 m/s
- Betrieb mit offener Schutztür mit Robotergeschwindigkeit 0 m/s < v < 4 m/s
- Betrieb mit inaktiver Zuhaltung mit Robotergeschwindigkeit 0 m/s < v < 4 m/s
- Betrieb mit offener Schleuse bei Robotergeschwindigkeit 0 m/s < v < 4 m/s und Transportbandgeschwindigkeit 0 m/s < v < 2 m/s
- Betrieb mit offener Schleuse bei Robotergeschwindigkeit <2 m/s und Transportbandgeschwindigkeit 0 m/s < v < 2 m/s

Bei der Andockstation ergeben sich 2 Szenarien:

- Betrieb bei Detektion eines Werkstücks am Eingang mit einer Transportbandgeschwindigkeit 0 m/s < v < 2 m/s
- Betrieb bei Detektion eines Werkstücks am Ausgang mit einer Transportbandgeschwindigkeit 0 m/s < v < 2 m/s

Bei dem Transportsystem ergibt sich folgendes Szenario:

- Detektion eines Werkstücks am Ausgang bei einer Transportbandgeschwindigkeit 0 m/s < v < 2 m/s

Die Aufgabe des Agenten zur dynamischen Schnittstellenfreigabe liegt nun darin, die sich aus den Entscheidungsbäumen der Einzelmodule ersichtlichen Risiken der Schnittstelle zuzuordnen und eine Parameterkonfiguration zu finden, bei welcher die detektierten Risiken durch die Interaktion mit der Umwelt beherrscht werden.

5.5.1 „Federmodul“/“Andockstation“

Die erste Schnittstellenüberprüfung bezieht sich auf den Betrieb des Federmoduls bei offener Schleuse, einer Transportbandgeschwindigkeit 0 m/s < v < 2 m/s und einer Parameterraumkonformen Robotergeschwindigkeit, sowie dem Betrieb der Andockstation bei Detektion eines Werkstücks am Eingang mit einer Transportbandgeschwindigkeit 0 m/s < v < 2 m/s. Der Schnittstellenagent benötigt hierbei genaue Informationen zu dem mechanischen Risiko und zu dem mechanischen Aufbau der beiden Module.

Um eine positive Schnittstellenüberprüfung sicher zu stellen ist es somit notwendig, dass dem Risiko-Reduzierungs-Agenten zur Risikobeurteilung die konstruktiven Übereinstimmungen der Transportbänder sowie deren Relativgeschwindigkeiten bekannt sind und überprüft werden.

5.5.2 „Andockstation“/“Transportsystem“

Die zweite Schnittstellenüberprüfung bezieht sich auf den Betrieb der Andockstation bei Detektion eines Werkstücks am Ausgang und einer Transportbandgeschwindigkeit 0 m/s < v < 2 m/s, sowie dem Betrieb des Transportsystems bei Detektion eines Werkstücks am Ausgang und einer Transportbandgeschwindigkeit 0 m/s < v < 2 m/s.

Zur positiven Schnittstellenüberprüfung ist es somit notwendig, dass der Risiko-Reduzierungs-Agenten zur Risikobeurteilung die Ausrichtung der Transportbänder zueinander überprüft. Dies kann mittels eines Vision-Systems auf der Andockstation des FTS erfolgen, welches neben der Ausrichtung der Transportbänder auch die Position des Transportsystems mittels Umwelterkennung überprüft. Nach entsprechender Schnittstellenüberprüfung mit positivem Ergebnis erfolgt die Freigabe.

6. Quellen

[WIKI19]: https://de.wikipedia.org/wiki/Komplexes_System

[STÜTT02]: Manfred Stüttgen: Komplexe adaptive Systeme - oder: was wir von der Komplexitätstheorie für die Organisation von Unternehmen lernen können. In: Peter Milling (Hrsg.): Entscheiden in komplexen Systemen. Berlin 2002, ISBN 3-428-09365-8, S. 333–348

[LIGG17]: P. Liggesmeyer, M. Trapp, "Safety in der Industrie 4.0: Herausforderungen und Lösungsansätze", in Handbuch Industrie 4.0 Bd.\, 1: Produktion, 2 ed. B. Vogel-Heuser, T. Bauernhansl, M. ten Hompel, Eds., Berlin: Springer, 2017, pp. 107-123.

[SF18]: Safety an modularen Maschinen; Whitepaper SF-3.1: 04/2018

[VDI/VDE 2653 Blatt1]: Agentensysteme in der Automatisierungstechnik - Grundlagen