# Smart Safety

## Automatisch Safety bewerten, flexibel produzieren

Industrie Service

**Mehr Wert.**
**Mehr Vertrauen.**

Fachaufsatz

Durch geringe Losgrößen bis hin zu Einzelanfertigungen variiert der Produktionsprozess modularer Anlagen häufig, auch die Gefahr für häufigere Stillstände steigt dadurch. Dieser Umstand erfordert eine sicherheitstechnische Neubewertung der Anlage. Ein automatisches Safety-Bewertungskonzept reduziert Stillstandzeiten und das bei einem unverändert hohen Sicherheitsniveau. TÜV SÜD hat mit der Initiative SmartFactoryKL das Konzept weiterentwickelt.

TÜV SÜD Industrie Service GmbH

Bei wesentlichen, sicherheitsrelevanten Änderungen am Maschinenverbund muss die CE-Konformität derzeit manuell bewertet werden. Um heute eine modulare Produktion zu ermöglichen, werden deshalb alle Varianten und Konfigurationen im Voraus betrachtet, bewertet und validiert. Das setzt voraus, dass alle Module mitsamt ihren sicherheitstechnischen Eigenschaften und Wechselwirkungen bekannt sind.

Für eine flexible Produktion im Sinne von Plug-&-Produce ist das ein Hemmnis. Denn durch die ständig wechselnden Anforderungen ist nicht vorhersehbar, welche Anlagenkonfigurationen zukünftig gebraucht werden. Mitunter bedeutet das, im laufenden Betrieb Maschinen einzubinden, die zum Zeitpunkt der Planung noch unbekannt sind.

Damit ist ein Konflikt zwischen den Zielen der Automatisierungstechnik und der Sicherheitstechnik entstanden. Derzeit angewandte Sicherheitskonzepte zum Schutz von Menschen und Investitionsgütern analysieren definierte Prozesse und sichern sie durch statische Lösungen ab. Dem entgegen steht das Ziel, flexibel auf unterschiedliche Anforderungen reagieren und dynamische Prozesse abbilden zu können. Zusammen mit dem Primärziel der Safety, Menschen nicht zu verletzen, bilden maximale Verfügbarkeit und die Einhaltung von Systemgrenzen ein komplexes Zielsystem. Daher ist eine neue Sicherheitsarchitektur nötig, die Hersteller sowie Betreiber bei der Bewertung sicherheitsrelevanter Zusammenhänge unterstützt.

## Mit Agenten die Komplexität beherrschen

Die einzelnen Module einer verketteten Anlage können vollständig beschrieben werden und sind sicherheitstechnisch beherrschbar. Im gemeinsamen Betrieb ergeben sich jedoch komplexe Wechselwirkungen die in der Planung nicht immer vorhersehbar sind. Hinzu kommen unterschiedliche Umweltbedingungen oder veränderliche Prozessbedingungen. Software – in Form von Agentensystemen – kann dazu eingesetzt werden, die daraus entstehenden Probleme bei der sicherheitstechnischen Betrachtung zu überwinden.

In den Agenten sind die Ziele und Fähigkeiten sowie die Informationen über den Zustand des jeweiligen Moduls integriert. Durch die Kommunikation untereinander kann das Agentensystem flexibel auf unterschiedliche Problemstellungen im Betrieb reagieren. Es müssen nicht alle möglichen Abläufe bereits beim Entwurf des Systems bekannt sein, denn die wesentlichen Eigenschaften des Gesamtverhaltens werden zur Laufzeit erfasst. Dadurch verfügt das Agentensystem jederzeit über alle sicherheitsrelevanten Informationen der Gesamtanlage.

Agentensysteme sind in der Automatisierungstechnik nicht neu. In VDI/VDE 2653 Blatt 3 werden verschiedene Szenarien vorgestellt und explizit der Einsatz in modularen Produktionsanlagen genannt. Die konzeptionelle Aufteilung on Funktionalitäten, Zielen und Entscheidungsprozessen auf autonome Einheiten ermöglicht eine systematische Dekomposition der Komplexität. So lässt sich eine automatische Safety-Bewertung in zwei Schritten realisieren.

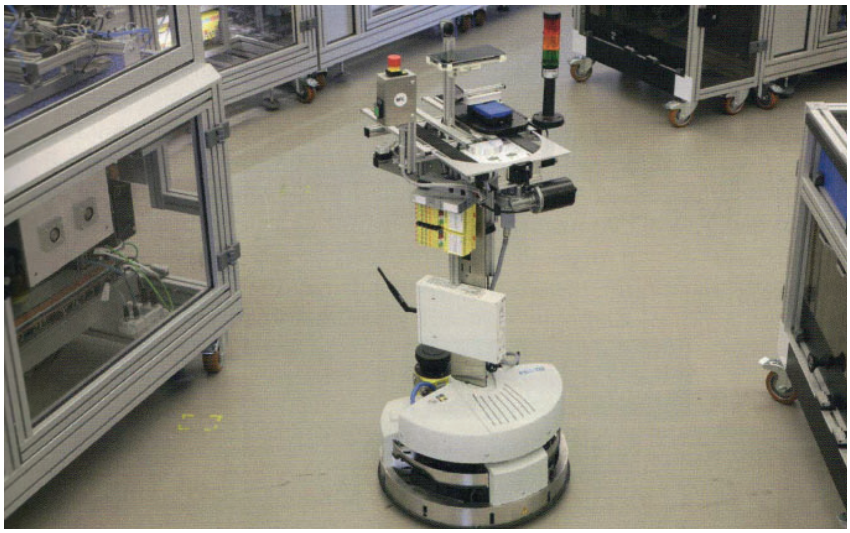

Abbildung 1: Das Fahrerlose Transport-System (FTS) wird über die Mobilfunk-technologie SG gesteuert.

## Dynamische Freigabe der Module

Die möglichen Safety-Zustände des Maschinenmoduls können vom Hersteller bereits bei der Entwicklung anhand von Parameterräumen definiert und in Form eines Entscheidungsbaumes manipulationssicher in der Verwaltungsschale abgelegt werden. Das umfasst beispielsweise die Geschwindigkeit eines Förderbandes oder den Zustand einer Sicherheitsschleuse. Die Entscheidungsbäume werden von der Risikobeurteilung des einzelnen Maschinenmoduls abgeleitet.

Die Enden („Blätter“) des Entscheidungsbaumes entsprechen dabei den möglichen Risiken bei den jeweiligen Prozessparametern. Beim Betrieb außerhalb der Parameterräume entzieht der Agent sofort die Freigabe und das Modul steht still.

Endet ein Pfad mit einem nicht tolerierbaren Restrisiko, werden die vorhandenen Sicherheitsprofile aus der Verwaltungsschale abgerufen und dem gegenübergestellt. Wenn die dort definierten Sicherheitseinrichtungen als geeignete Safety-Maßnahmen bewertet werden, erfolgt die Freigabe. Sind sie nicht ausreichend oder steht kein entsprechendes Sicherheitsprofil zur Verfügung, wird die Freigabe für die eingestellten Parameter entzogen.

Sowohl die erteilten als auch die entzogenen Freigaben werden ebenfalls sicher in der Verwaltungsschale abgelegt und stehen somit für künftige Risikobewertungen zur Verfügung. Bei einer negativen automatischen Bewertung ist zudem eine manuelle Nachbewertung durch einen autorisierten Safety-Experten möglich.

Mit diesem Konzept kann der Betreiber eine flexible Fertigung bei im Vorfeld unbekannten Prozessen realisieren, ohne die Vorgaben des Arbeitsschutzgesetzes zu verletzen.

## Bewertung der Schnittstellen

Zur Bewertung der Schnittstellen zwischen den einzelnen Produktionsmodulen werden nicht die jeweils eingestellten Parameter betrachtet, sondern die ermittelten Risiken. Diese ergeben sich aus den Blättern der Entscheidungsbäume der Einzelmodule, denen kein entsprechendes Sicherheitsprofil entgegensteht. Der Grund dafür ist, dass dem Hersteller in der Entwicklungsphase die Umweltbedingungen im Einsatz unbekannt sind. Anstatt einen bestimmungsgemäßen Gebrauch zu definieren, wird deshalb versucht, die Sicherheit des Anlagenverbundes durch die Kombination der einzelnen dynamischen Freigaben und der Schnittstellenbewertung festzustellen.

Um die Freigabe der Schnittstelle zu überprüfen, identifiziert ein Risiko-Reduzierungsagent die Gefahren und versucht eine Parameterkonfiguration zu finden, bei der sie beherrscht werden. Dafür muss der Agent auf die konstruktiven Eigenschaften sowie die aktuellen Betriebsparameter und Safety-Daten zugreifen können, beispielsweise über den digitalen Zwilling in der Verwaltungsschale. Gegebenenfalls können auch Sensoren und Systeme zur Umwelterkennung herangezogen werden.

Die Risiko-Reduzierungsagenten an der Schnittstelle bilden dadurch eine zusätzliche Datenbasis für die Interaktion mit dem Umfeld. Sie können die Notwendigkeit eines Sicherheitsprofils für bestimmte Zustände aufheben, indem ihre Ausgaben den Risiken gegenübergestellt werden, denen sonst kein gültiges Sicherheitsprofil innerhalb der Module entspricht.

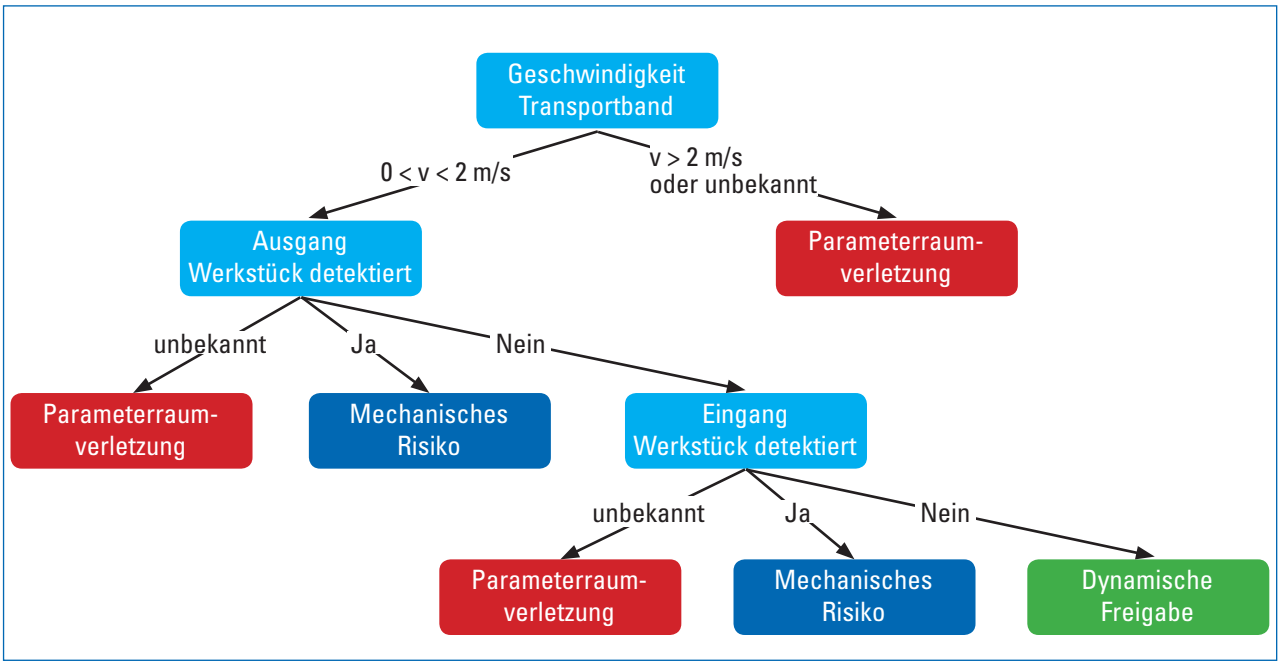


Abbildung 2: Entscheidungsbaum Andockstation für das Beispiel „Transportsystem“.

## Use-Case: Transportsystem und Andockstation

Innerhalb der SmartFactoryKL transportiert ein Fahrerloses Transportsystem (FTS) Werkstücke zwischen den verschiedenen Produktionslinien (s. Abbildung 1). Es verfügt über zwei Förderbänder und einen Sensor, der die Aufnahme des Transportguts erkennt. Innerhalb der Anlage interagiert das FTS mit einer Andockstation, um die Werkstücke auszutauschen. Beide Akteure werden als eigensichere Module angesehen.

Dabei handelt es sich zwar um eine vergleichsweise einfache Safety-Aufgabenstellung, sie zeigt jedoch, dass mit dem vorgestellten Konzept der Anlage zuvor unbekannte Maschinenmodule zur Laufzeit hinzugefügt werden können.

Für das Transportsystem werden zwei Parameter des Parameterraumes als Beispiel hier aufgeführt:

- Geschwindigkeit der Transportbänder: 0-2 Meter pro Sekunde (in Abhängigkeit vom Werkstück festgelegt)
- Werkstück erkannt: Ja/Nein

Die Parameterräume sind im digitalen Zwilling des Transportsystems gespeichert und werden in Echtzeit abgeglichen. Sie bilden die Datenbasis für die Bewertung durch den Risiko-Reduzierungsagenten. Überschreitet das Transportband fehlerhafterweise die zulässige Geschwindigkeit oder fällt der Sensor aus (ein Werkstück wurde nicht eindeutig erkannt), stellt das eine Parameterraumverletzung dar – die Freigabe wird entzogen und das FTS steht still. Die dynamische Freigabe erfolgt, wenn nichts befördert wird. Der Transport eines Gegenstands stellt immer ein mechanisches Risiko dar und ist nur nach der Überprüfung der Schnittstellen möglich.

Die Andockstation der SmartFactoryKL besitzt ebenfalls zwei gegenläufige Förderbänder, die ein Werkstück vom angrenzenden Modul zum Ende der Produktionslinie oder in die Gegenrichtung transportieren. Sensoren erkennen die Werkstücke am Ein- oder Ausgang. Zulässige Parameterräume sind beispielsweise:

- Geschwindigkeit der Transportbänder: 0-2 Meter pro Sekunde (in Abhängigkeit vom Werkstück festgelegt)
- Werkstück am Ausgang erkannt: Ja/Nein
- Werkstück am Eingang erkannt: Ja/Nein
- Der Entscheidungsbaum, der innerhalb des Agenten der Andockstation ausgeführt wird, ist für dieses Beispiel in Abbildung 2 dargestellt.

Der produktionstechnische Betrieb der Andockstation ist automatisch freigegeben, wenn nichts befördert wird. Ein Werkstück am Eingang oder Ausgang bedeutet ein (mechanisches) Risiko – beispielsweise durch Herabfallen. Das heißt, dass der Agent zusätzlich die Schnittstelle zwischen dem Fahrerlosen Transportsystem und der Andockstation bewerten muss, wenn sie Werkstücke austauschen. Dafür überprüft er mithilfe eines Vision-Systems die Ausrichtung der Transportbänder zueinander und die Position des FTS. Bei einem positiven Ergebnis erteilt der Agent die Freigabe und die beiden Module können das Werkstück übergeben bzw. austauschen.

## Fazit

Dem Einsatz Künstlicher Intelligenz in der Maschinensicherheit stehen Vorbehalte gegenüber. Daher ist schon mit Beginn der Sicherheitsplanung eine fundierte Nachweisführung und eine umfangreiche Validierung notwendig. Mit diesem Konzept können die Schnittstellenkomplexität von verketteten Anlagen beherrscht und Stillstandzeiten reduziert werden.

Eine standardisierte, herstellerunabhängige Semantik zur Beschreibung der Risiken und Sicherheitsprofile ist dafür unbedingt notwendig. Nur so können Module von unterschiedlichen Herstellern in einen Maschinenverbund integriert werden und die verschiedenen Safety-Agenten untereinander kommunizieren. Damit wird die Basis für den sicheren Einsatz adaptiver Safety-Lösungen innerhalb dynamischer Prozesse gelegt.

## SmartFactoryKL

Die SmartFactoryKL ist ein Netzwerk von rund 50 Akteuren aus Industrie und Wirtschaft. Diese Partner führen gemeinsame Forschungs- und Entwicklungsprojekte rund um die Industrie 4.0 und die Fabrik der Zukunft durch. Die Arbeit reicht von der Entwicklung und Beschreibung ihrer Vision bis hin zur industriellen Realisierung. Als unabhängige Organisation ist das Netzwerk eine neutrale Plattform.

Herzstück der inhaltlichen Arbeit des Netzwerks bildet die weltweit einzigartige, herstellerunabhängige Demonstrations- und Forschungsanlage – die Industrie 4.0-Produktionsanlage des SmartFactoryKL-Partnerkonsortiums. Hier bringen Forscher und Praktiker die Ideen von Industrie 4.0 gemeinsam voran. Innovative Informations- und Kommunikationstechnologien werden in realitätsnahen industriellen Produktionsumgebungen getestet und weiterentwickelt. So werden ausgereifte Informationstechnologien in die Fabrikautomation integriert.

Die Module der Industrie 4.0-Anlage des SmartFactoryKL-Partnerkreises verteilen sich auf vier Fertigungsinseln, um eine flexible Produktion zu ermöglichen.

## Autoren

**Michael Pfeifer**
Sachverständiger für Maschinen- und Anlagensicherheit

TÜV SÜD Industrie Service GmbH
80686 München
michael.pfeifer@tuev-sued.de

**Werner Varro**
Teamleiter Industrieelektronik

TÜV SÜD Product Service GmbH
80686 München
werner.varro@tuev-sued.de



TÜV SÜD Industrie Service GmbH
80686 München

Telefon 089 5791-3329
michael.pfeifer@tuev-sued.de

www.tuev-sued.de/is

TÜV SÜD Product Service GmbH
80339 München

Telefon 089 50084-529
werner.varro@tuev-sued.de

www.tuev-sued.de/ps