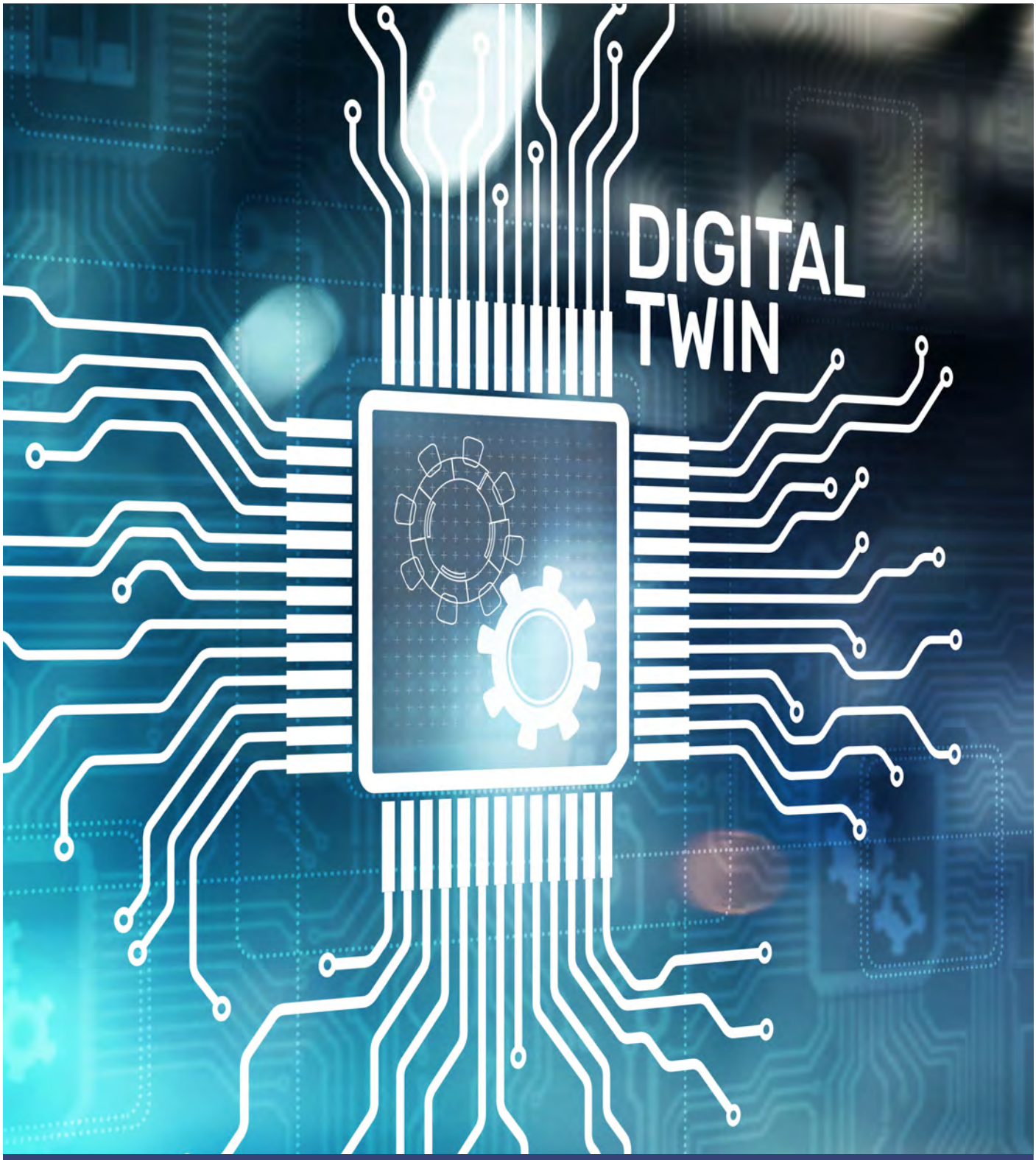

Smart Safety – Das Konzept Knowledge Graph zur Umsetzung von Safety in Digitalen Zwillingen

Whitepaper SF-3.4: 05/2022

smartFactory KL®

Abstract
Das Thema Safety in modularen Industrie 4.0-Produktionsanlagen wird im Rahmen der Arbeitsgruppe 2 „Connect & Control" der ***SmartFactory***^{KL} vorangetrieben. Die Safety-Architektur der ***SmartFactory***^{KL} beinhaltete bisher die Kernkomponenten der modularen Zertifizierung, den digitalen Zwilling sowie eine entscheidungsbaumbasierte Risikobewertung, welche in den Vorgängerarbeiten beschrieben wurden. Die Kombination und Vernetzung von Komponenten, Aspekten und Informationen werden im Zuge der aktuellen Arbeiten der Arbeitsgruppe durch den Einsatz von Knowledge Graphen verbessert und daraus Synergien und weitere Potenziale geschaffen. Der Einsatz des Knowledge Graphen als zentrale Komponente der Safety-Architektur ermöglicht die realitätsabbildende Verknüpfung von multimodalen Zusammenhängen sowie komplexer Fachlichkeit. Durch diese Weiterentwicklung der Safety-Architektur wird unter anderem eine Erhöhung der Autonomie und Flexibilität in der Gefährdungserkennung nach einer Anlagenänderung und damit in der Risikobewertung, aber auch in der Gefährdungsbeurteilung erreicht. Dies wird anschaulich in Form eines Use-Cases dargestellt.

Keywords
Smart Safety, Knowledge Graph, Entscheidungsunterstützung, Risikobewertung, Modulare Produktion, Flexible Produktion, Industrie 4.0

Autoren

Michael Pfeifer	TÜV SÜD Industrie Service GmbH
Dimitri Harder	TÜV SÜD Product Service GmbH
Dr. Detlev Richter	TÜV SÜD Product Service GmbH
Klaus Reichenberger	Empolis Information Management GmbH
Bernd Neuschwander	Pilz GmbH & Co. KG
Matthias Schweiker	Pilz GmbH & Co. KG
Alexander David	DFKI GmbH
Pascal Rübel	DFKI GmbH
Manuel Heid	DFKI GmbH
Dr.-Ing. Achim Wagner	DFKI GmbH
William Motsch	Technologie-Initiative ***SmartFactory***^{KL}
Prof. Dr.-Ing. Martin Ruskowski	Technologie-Initiative ***SmartFactory***^{KL}.

Inhaltsverzeichnis

[1] In diesem Papier wird der neutrale Term digitaler Zwilling verwendet, da Funktionalitäten diskutiert werden, die bisher bspw. in der Standardisierung zur Verwaltungsschale bisher nicht beschrieben werden.

1. Zielsetzung des Whitepapers

Dieses Whitepaper fasst die aktuellen Ergebnisse der Arbeitsgruppe **Safety** in dem modularen Cyber-Physischen Produktionssystem der ***SmartFactory***^{KL} zusammen. In Zusammenarbeit mit den beteiligten Partnern **TÜV Süd, Empolis, PILZ** und **DFKI** wird die bisherige Safety-Architektur um den Baustein des Knowledge Graphen erweitert. Somit können die komplexe Fachlichkeit und multimodale Zusammenhänge zielführend verknüpft werden. Das im Whitepaper 2020 dargestellte Zusammenspiel mit digitalen Zwillingen [1] rundet den neuen Architekturbaustein ab.

Ziel dieses Whitepapers ist es das Safety-Konzept für leicht wandelbare, modulare Produktionsanlagen unter Einbeziehung der Erkenntnisse aus bisherigen Arbeiten mit dem Ansatz zur Risikobewertung mit Entscheidungsbäumen [2] und der modularen Zertifizierung [3] weiter zu entwickeln und mit der Einbindung neuer Lösungsansätze, bspw. des Knowledge Graphen, die Umsetzbarkeit weiter voranzutreiben. Hierbei sollen die Vorteile des Einsatzes von Knowledge Graphen und damit die Weiterentwicklung der bisherigen Konzepte aufgezeigt werden, welche die Komplexität von Safety kontextbezogen und wissensbasiert abbilden können. Der aufgeführte Use-Case, welcher aus dem realen Produktionsumfeld aufgegriffen wurde, veranschaulicht die theoretischen Überlegungen in der Praxis.

Kommende Aktivitäten der Arbeitsgruppe Safety sind insbesondere die Implementierung **im Sinne eines agentenbasierten verteilten Ansatzes** und die systematische Ausarbeitung einer am Demonstrator orientierten **Safety-Ontologie** und anknüpfender **Semantik**.

2. Motivation

Hohe Variantenvielfalt, individuelle Produkte und kürzere Produktlebenszyklen führen zu kleineren Produktvolumina und kleineren Losgrößen in der Fertigung. Um die geforderte höhere Flexibilität zu erreichen, sind nicht nur Fertigungskonzepte wie die modulare Produktion und Plug & Produce unabdingbar, sondern es werden auch Bewertungskonzepte für die Maschinen- und Anlagensicherheit (im Weiteren Safety genannt) benötigt, die den Randbedingungen modularer und flexibler Produktionssysteme gerecht werden.

Da nahezu jede neue Anlagenkonfiguration und -parametrierung eine veränderte Gefahrensituation mit sich bringen kann, wird eine entsprechende Safety-Bewertung inklusive festgelegter Schutzmaßnahmen benötigt, bevor mit der Produktion begonnen werden darf. Konventionelle Safety-Ansätze kommen dabei aufwandsmäßig an ihre Grenzen. Der statische Aufbau der Konzepte bringt zwar einen hohen Sicherheitsfaktor mit sich, die unterschiedlichen Anforderungen verschiedener Situationen können allerdings nur eingeschränkt berücksichtigt werden, so dass es üblich ist mit Worst-Case-Szenarien zu arbeiten. Dies kann an vielen Stellen zu stark reduzierten Geschwindigkeiten und vermeidbaren Stopps führen.

Die von Experten durchgeführten Bewertungen sind jedoch aufwändig und erfordern viel Zeit, insbesondere bei technisch immer komplexer werdenden Maschinen. Eine Beschleunigung der Bewertungsprozesse, besonders durch die höhere Anzahl der Veränderungen, ist essenziell für eine konkurrenzfähige Produktivität. Die Beschleunigung kann sowohl durch eine Optimierung manueller Verfahren als auch durch die Einführung (teil-)automatisierter Prozesse erreicht werden. Bei jeglichen Veränderungen am Konzept der Safety-Bewertungen hat die Vollständigkeit und Wirksamkeit der Bewertung und einhergehender Schutzmaßnahmen höchste Priorität.

Der bereits angesprochene Freigabeprozess ist dabei heutzutage ein hochgradig manueller Prozess, der weitestgehend ohne technische Hilfsmittel durchgeführt wird. Meist kommen dabei Vorlagen zum Einsatz, die zum einen oft nicht den gesamten Prozess, sondern nur Teile abdecken, zum anderen aber auch vom jeweiligen Servicepersonal unterschiedlich interpretiert und eingesetzt werden. Zudem ist für die risikotechnische Beurteilung einer Anlage auch ein tiefgehendes technisches Verständnis von Nöten, um komplexe Zusammenhänge zu erfassen und dadurch richtig zu beurteilen. Fehlendes Fachwissen, bspw. zur Cybersecurity in vernetzten Produktionsanlagen, kann hierbei dazu führen, dass Risiken falsch bewertet oder gar übersehen werden.

Die sicherheitstechnische Bewertung einer Anlage kann dabei je nach Komplexität zwischen einigen Tagen und im Bereich von Wochen dauern. Unter anderem müssen die Risiken vor Ort erfasst und im Nachgang bewertet werden. Daran anschließend folgt eine Minderung der erfassten Risiken. Ein großes Hindernis ist dabei das Fehlen bzw. das unvollständige Vorliegen von Unterlagen und Dokumenten, da meist verschiedene Fachbereiche einer Firma, oder gar aus verschiedenen Firmen, Informationen miteinander teilen bzw. zur Verfügung stellen müssen. Hierbei spielt das Fehlen einer Austauschplattform bzw. der fehlende Zugriff darauf ebenfalls eine Rolle. Der fehlende Zugriff auf Informationen wird nicht selten mit dem Schutz von geistigem Eigentum oder anderen rechtlichen Randbedingungen begründet. So legen Maschinenhersteller ihre detaillierten Unterlagen häufig nur den Partnerunternehmen offen, die sie bei der Erstellung der Risikobeurteilung oder des Handbuchs unterstützen. Digitale Zwillinge können helfen, den Informationsaustausch zu verbessern, da die unter geistigem Eigentum stehenden Unterlagen nicht offengelegt werden, sondern lediglich ausgewählte Informationen hinterlegt werden.

Jede assistierte oder automatisierte Funktion führt zusammenfassend direkt zu einer Effizienzsteigerung. Jegliche einheitliche und ganzheitliche Checkliste, die den kompletten Prozess und nicht nur Teile davon abdeckt, bis hin zu einer assistierten bzw. automatisierten Unterstützung von 50%, 60% oder gar 70% hat dabei einen direkten Einfluss auf den Aufwand der Safety-Bewertung des Freigabeprozesses. Diese kann direkt in einer Wirtschaftlichkeitsrechnung betrachtet, bewertet und mit einbezogen werden.

Sowohl technische Ansprüche wie eine gute Anpassbarkeit an neue Konfigurationen mit Erkennung ggf. neuer Gefahren und das flexible Handling auftretender Restrisiken, als auch wirtschaftliche Aspekte wie Anlageneffizienz und Beschleunigung von Sicherheitsfreigaben stellen Safety-Konzepte vor neue Herausforderungen. Anschauliche Anwendungsszenarien werden in diesem Whitepaper genauso diskutiert wie mögliche Lösungsansätze, welche die nötige Flexibilität bei gleichzeitiger kompromissloser Sicherheit herstellen können.

3. Theoretische Grundlage

3.1 Weiterentwickelter Lösungsansatz: Architektur in der Smart Factory [KL]

Mit dem Whitepaper 2019 [2] wurde der Entscheidungsbaum als möglicher Ansatz für die Identifizierung relevanter Gefährdungen verketteter modularer Maschinenanlagen vorgestellt. Im Rahmen der weiteren Entwicklungstätigkeiten zeichneten sich schnell deutliche Schwächen dieses Lösungsansatzes ab. Insbesondere bei Maschinenanlagen mit hohem Komplexitätsgrad würden sich sehr große und nur noch schwer überblickbare Entscheidungsbäume ergeben. Das ist ein Aspekt, der unter Gesichtspunkten der Qualitätssicherung, Nachvollziehbarkeit und Überprüfbarkeit als nicht zielführend bewertet wurde. Ein weiterer Nachteil ist die Starrheit von Entscheidungsbäumen, die eine Anpassungsfähigkeit an neue Konfigurationen im Sinne von Plug & Produce nur mit besonderen Aufwänden ermöglicht hätte. Ein Gesamtkonzept bestehend aus digitalen Zwillingen und Knowledge Graph hat sich hingegen als zielführend herausgestellt.

Der Knowledge Graph kommt dabei auf Maschinen- und Systemebene zum Einsatz, d.h. innerhalb eines digitalen Zwillings einer Maschine und in der Interaktion zwischen digitalen Zwillingen.

Im eingesetzten Knowledge Graphen werden sogenannte Safety Rules sowie Hazard Rules und deren Interdependenzen modelliert. Hazard Rules stellen dabei die Beziehungen zwischen Parametern dar, die bei Zusammenkunft dazu führen, dass ein Safety-Experte von einem bestimmtem Hazard (Gefährdung) spricht, vgl. „Problem hinter einer Gefahr“ [1]. Gleichzeitig wird durch die Safety Rules ausgedrückt, welche Parameter von einer Schutzmaßnahme beherrscht oder negiert werden. Sie ermöglichen somit das „Matching“ zwischen verfügbaren Schutzmaßnahmen und einer konkreten Gefährdung.

Gleichzeitig wird durch das Erfüllen einer Hazard Rule und dementsprechend mit der Identifikation einer Gefährdung die situative Risikobeurteilung ausgelöst. Eine solche situative Risikobeurteilung kann im Rahmen der virtuellen Inbetriebsetzung (IBS) bei der Safety Simulation oder im Rahmen der Produktion zur Laufzeit ablaufen. Eine weitere Möglichkeit ist der Ablauf als sogenannte „Predictive Safety“. Dabei werden vorausschauend Gefährdungssituationen bewertet und frühzeitig Schutzmaßnahmen zur Vermeidung von Safety-Stops eingeleitet, welche durch die konventionelle Funktionale Sicherheit ausgelöst werden können sowie die Produktivität hemmen. Grundsätzlich laufen die Risikobewertungen vergleichbar ab. Der Unterschied einer situativen zu einer konventionellen Risikobewertung besteht darin, dass anstatt Worstcase-Annahmen, die situativ aktuellen Parameter einbezogen werden.

Gemäß DIN EN ISO 12100 [4] ist das Risiko (bezogen auf die betrachtete Gefährdung) eine Funktion von Schadensausmaß (das aus der betrachteten Gefährdung resultieren kann) und Eintrittswahrscheinlichkeit dieses Schadens (Gefährdungsexposition einer Person/ Personen, Eintritt eines Gefährdungsereignisses, Möglichkeit zur Vermeidung oder Begrenzung des Schadens).

Eine situative Risikobeurteilung wird durch einfache Beispiele in diesem Dokument veranschaulicht.

3.2 Erklärung: Knowledge Graph – transparente und nachvollziehbare Darstellung von komplexen Zusammenhängen

Knowledge Graphen repräsentieren Wissen als Verknüpfungen zwischen Objekten, wobei die unterschiedlichen Typen von Objekten und Verknüpfungen (auch Relationen genannt) eine wichtige Rolle spielen: In unserem Beispiel in Abbildung 1 sind Objekte vom Typ „Fehler" durch die Relation „tritt auf bei" mit Objekten vom Typ „Bauteil" verknüpft. Bauteile „sind Bestandteil" von anderen Bauteilen oder von Produkten und können nicht nur von Fehlern, sondern auch von Maßnahmen, etc. betroffen sein. Zusätzlich können Objekte Attribute haben: in unserem Beispiel haben Bauteile eine Abmessung und einen Preis sowie Maßnahmen eine Dauer.

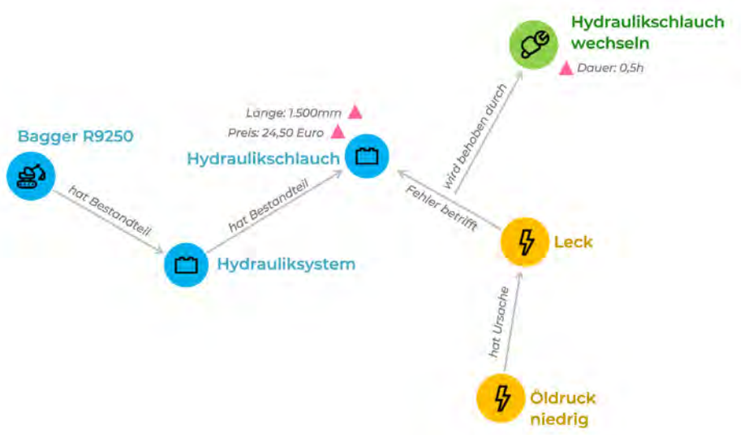

Abbildung 1: Produkte, Bauteile, Fehler und Maßnahmen in einem Knowledge Graph

Die Vernetzung wird um Mechanismen zur Ableitung von Wissen, das Ziehen von Schlussfolgerungen und der Vererbung von Informationen erweitert. Dies wird an folgendem einfachen Beispiel dargestellt: Das Objekt Bagger R9250 "hat Bestandteil" Hydrauliksystem, das Hydrauliksystem "hat Bestandteil" Hydraulikschlauch, also ist der Hydraulikschlauch auch ein Bestandteil des Bagger R9250. Damit beschränken sich Knowledge Graphen nicht darauf, einfach nur Daten aufzunehmen und wiederzugeben. Sie bilden die Logik einer Domäne, z.B. einer Industrieanlage, in einem formalen Modell ab. In diesem Modell können Fälle durchgespielt und in ihren Abhängigkeiten bewertet werden.

Anforderung Modular Safety: Multidimensionale Abhängigkeiten abbilden

Graphen können von allen Seiten betrachtet werden – es kann mit der gleichen Leichtigkeit eine Komponente ins Zentrum gestellt werden, wie ein Fehler oder eine Maßnahme. Aus Sicht des Produkts können alle möglichen Fehler aufgelistet werden oder umgekehrt bei einem Fehler alle Bauteile aufgeführt werden, die von diesem Fehler betroffen sein können, sowie alle Produkte, in die diese Bauteile eingebaut sind. Die eingebaute Vererbung und die Fähigkeit Schlussfolgerungen zu treffen, machen es im Knowledge Graph vergleichsweise leicht auch für komplexe Situationen die Sicherheitsimplikationen zu ermitteln.

Anforderung Modular Safety: Komplexe Fachlichkeit

Knowledge Graphen sind nachvollziehbare Modelle, da sie ihre Schlussfolgerungen und Empfehlungen (z.B. vorhandene Risiken und mögliche Maßnahmen) jederzeit verständlich begründen können. Damit unterscheiden sie sich von den typischen Black-Box-Modellen des Machine Learning. Dementsprechend werden sie nicht allein durch Training mit vielen Beispieldaten aufgebaut, sondern repräsentieren explizites Expertenwissen. Insbesondere für Safety-Anwendungen ist diese Kombination essenziell, da durch Expertenwissen im Vorfeld gefährliche Situationen ad hoc erkannt und nicht zugelassen werden. Somit tauchen sie auch nicht in einer Datenbasis auf und finden daher im Weiteren in gelernten Modellen keinen Einbezug.

Dafür ist es besonders wichtig, dass Knowledge Graphen einfach verständlich für die Nutzer sind – nicht nur für IT-Experten, die mit der Erstellung von Applikationen vertraut sind. Anders als gespeicherte Werte in einer Tabellenzelle werden durch die Vernetzung im Knowledge Graph Daten anschaulich repräsentiert.

Damit bieten sie bis tief in die technische Repräsentation der Daten hinein eine bessere Zugänglichkeit – Fachexperten können so direkt, schnell und einfach in die Entwicklung einbezogen werden.

Die Empolis-Knowledge-Graph-Plattform bietet gerade für komplexe technische Zusammenhänge eine große Ausdrucksmächtigkeit. So erlaubt sie beispielsweise auch Attributwerte und Relationen selbst wieder mit Relationen zu verknüpfen und kann so bedingte Aussagen adäquat repräsentieren, wie z.B.: „In diesem Betriebsmodus geht von der Komponente folgende Gefahr aus". Modelliertes Beziehungswissen kann ergänzt werden, durch dynamisches Regelwissen, wie beispielsweise: „Wenn der Abstand zwischen Komponente X und Y kleiner ist als die größte Ausdehnung des Werkstücks, dann besteht Einklemmgefahr". Die grafische Oberfläche und die intuitiven Visualisierungen der Empolis-Knowledge-Graph-Plattform sorgen dafür, dass auch derart komplexes Wissen von Fachexperten modelliert werden kann.

4. Das Konzept Knowledge Graph zur Umsetzung von Safety in Digitalen Zwillingen

Beim Lesen vieler Veröffentlichungen zu digitalen Repräsentanzen wird der Eindruck erweckt, dass die digitale Repräsentanz einer Maschine eine „lose" Sammlung von Daten und Informationen oder Datenblättern darstellt. Die Umsetzung von Plug & Produce aus Safety-Sicht zeigt jedoch, dass funktionale Zusammenhänge zwischen Parametern und Informationen bestehen, die auch in der Digitalen Repräsentanz abgebildet sein müssen. Es liegt somit nahe, die Idee der Nutzung eines Knowledge Graphen auf der Systemebene sinngemäß auf die Maschinenebene in den Digitalen Zwilling zu übertragen.

Das Beispiel eines Unfalls in Deutschland überträgt die obigen Szenarien in die reale Welt. Die ausgeschlagene Schutztür einer Drehmaschine war die Ursache für den tragischen Todesfall eines Bedieners, der in der Nähe der Maschine arbeitete. Es ist anzumerken, dass gemäß der einschlägigen Maschinennorm (ISO 23125 - Werkzeugmaschinen - Sicherheit – Drehmaschinen – Maschinen [5]) Schutztüren mit Rückhaltefunktion eine begrenzte mechanische Rückhaltefähigkeit aufweisen dürfen, die jedoch u.U. deutlich geringer als das maximal zulässige Werkstückaufnahmegewicht der Maschine ausfällt. Im beschriebenen Unfall war die Rückhaltefähigkeit der Schutztüre für das Backenfutter ausgelegt; die maximale Werkstücktragfähigkeit lag bei 400 kg. Aktuelle Safety-Praxis ist es, einen Hinweis in die Betriebsanleitung aufzunehmen, der den Betreiber darüber informiert: "Die Schutztür minimiert das Risiko des Herausschleuderns, schließt es aber nicht vollständig aus."

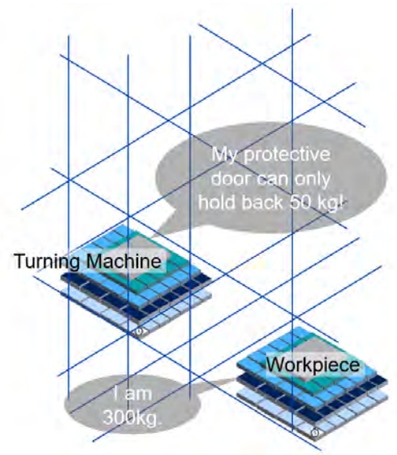

Abbildung 2: Interagierende digitale Repräsentanzen eines Werkstückes und einer Drehmaschine

Der Sicherheitshinweis in der Betriebsanleitung kann in der Praxis weniger wirksam sein als durch das Safety-Konzept vorgesehen, insbesondere bei der Handhabung und Benutzung von „Standard-Maschinen“ oder eben durch den „Lauf der Zeit“. Während im Rahmen der Inbetriebsetzung der Maschine die Betriebsanleitung zumindest teilweise gesichtet wird, zeigt die Praxis, dass insbesondere bei jahrelangem störungsfreiem Betrieb manche Hinweise in Vergessenheit geraten. Die Wahrscheinlichkeit, dass das menschliche Verhalten versehentlich zu unsicheren Praktiken übergeht, kann trotz regelmäßiger Unterweisungen nicht ausgeschlossen werden.

Ähnlich verhält es sich erfahrungsgemäß bei der Installation, Inbetriebsetzung und dem Betrieb von „Standard-Maschinen“, deren Bedienung „klar ist“ und die Sichtung der Betriebsanleitung seltener als erforderlich angesehen wird. Hinweise zu Restrisiken, wie vom Safety-Konzept vorgesehen, können somit nicht zur Kenntnis genommen und auch nicht im Zusammenhang mit den auf Betreiberseite implementierten zusätzlichen Schutzmaßnahmen, bspw. Maschinenausrichtung, Zugangsbeschränkungen oder persönliche Schutzausrüstung, bewertet werden.

In diesem Fall kann Smart Safety mit einer automatisierten Risikobewertung zur Laufzeit Abhilfe bieten. Denn das System hätte automatisch eine Warnung vor der gefährlichen Situation aus der Kombination Maschine und schwerem Werkstück an den Betreiber ausgegeben. Mögliche zusätzliche Schutzmaßnahmen könnten ein vorübergehend eingeschränkter Zugang zum betroffenen Gefahrenbereich, sichtbare oder akustische Warnungen, eine mobile Barriere oder andere geeignete Maßnahmen sein. Umgekehrt würde eine pauschale Festlegung dieser zusätzlichen Maßnahmen für alle Werkstücke keinen Sinn machen, da die Produktivität in ihrer Gesamtheit durch eine solche „Worstcase-Maßnahme“ zu stark beeinträchtigt würde.

In der Umsetzung im digitalen Zwilling sieht das Beispiel eines möglicherweise davonfliegenden Bauteils folgendermaßen aus: Wie im Whitepaper 2020 [1] mit „Problem hinter einer Gefährdung“ beschrieben, werden die Aspekte erfasst, die zu einer gefährlichen Situation führen. In nachfolgender Abbildung ist eine Visualisierung eines digitalen Zwillings dargestellt, die beispielhaft verschiedene funktionale Zusammenhänge zwischen Parametern analog wie ein Knowledge Graph darstellt. Die darin gezeigte Struktur dient der leichteren Nachvollziehbarkeit und Zuortbarkeit von einzelnen Aspekten oder Parametern.

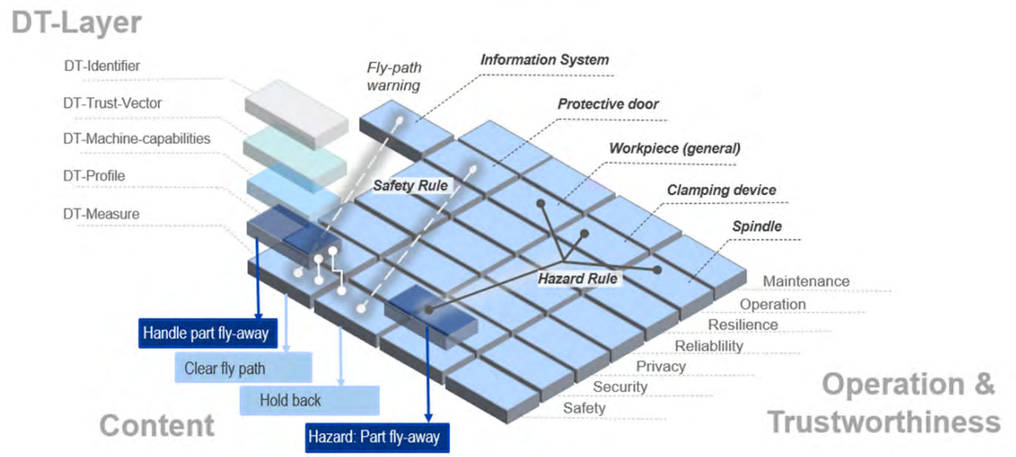

Abbildung 3 Grafische Visualisierung einer digitalen Repräsentanz einer Drehmaschine (Quelle: TÜV SÜD)

Das in das Backenfutter eingespannte Werkstück, welches mit der Spindel fest verbunden ist, „aktiviert“ bei Drehanforderung der Spindel die Gefahr „Herausschleudern“. Das Safety-Profil „Absicherung Herausschleudern“ ist beispielhaft mit der Schutzmaßnahme "Schutztüre" und "Gefahrenbereichswarnung" verbunden. Für Werkstücke, deren rechnerische kinetische Energie die Rückhaltefähigkeit der Schutztüre übersteigt, wird eine Warnung ausgesprochen, mit der Möglichkeit ergänzende Maßnahmen festzulegen, wie oben beschrieben.

Die vorher genannten Ausführungen zeigen, dass die Abbildung funktionaler Zusammenhänge zwischen Parametern und Informationen im Sinne eines Knowledge Graphen oder auch „Safety Rules“ genannt, das automatische Aufzeigen von situativ relevanten Gefährdungen, bspw. im Rahmen einer virtuellen Inbetriebsetzung während der Produktionsplanung oder sogar auch zur Laufzeit, ermöglicht.

Das Konzept von Smart Safety kann somit auf der einen Seite, durch das Aufzeigen von situativ relevanten Gefahren und Warnungen, helfen, das Sicherheitsniveau zu optimieren, insbesondere durch bessere Beherrschung der Schnittstellenproblematik. Auf der anderen Seite kann durch eine virtuelle Inbetriebsetzung mit digitalisierter Safety-Bewertung die optimale Anlagenkonfiguration gefunden werden. Eine digitalisierte Safety-Bewertung ermöglicht insbesondere für Produktionen

mit Anforderungen an Wandelbarkeit, Anpassungsfähigkeit und Flexibilität einen Wettbewerbsvorteil, da durch eine deutlich beschleunigte Safety-Bewertung die die Down-time reduziert werden kann. Eine Safety-Überwachung zur Laufzeit mit vorausschauender Funktion ermöglicht außerdem das frühzeitige Erkennen von gefährlichen Situationen, so dass alternative Maßnahmen aktiviert werden können, bevor die funktionale Sicherheit einen Safety-Stop auslöst. Dadurch sind geringere Stillstandzeiten und mehr Produktivität die Folge. Hierfür sind jedoch nicht nur digitale Abbildungen von Safety-Maßnahmen oder Gefahren erforderlich. Es müssen auch sämtliche Funktionen und Eigenschaften der Maschinen abgebildet vorliegen, denn für eine vorausschauende Safety sind nicht nur die klassischen Safety-Funktionen erforderlich, sondern auch betriebliche.

Vorausschauende Safety bedient sich auch betrieblichen Funktionen

Eine für die nahe Zukunft erkannte "gefährliche Situation" ergänzen: für eine Produktionsumgebung darf auch durch eine betriebliche Funktion entschärft werden, da die gefährliche Situation noch nicht eingetreten ist. Aus dem Umstand heraus, dass verschiedene Situationen unterschiedlich sind, ergeben sich unterschiedliche Maßnahmen für die Beherrschung, so dass die für die jeweilige Situation beste Maßnahme ausgewählt wird [2]. In diesem Rahmen wurde für die Maßnahmenauswahl bereits die Einbeziehung von Aspekten wie Einfluss auf die Produktivität und Verschleiß von Komponenten eingeführt. Ergänzend dazu wurde in diesem Whitepaper der Knowledge Graph für das Aufzeigen von Abhängigkeiten und Beziehungen implementiert. Je nachdem welche Beziehungen bzw. Zusammenhänge adressiert werden, wird von Safety Rules bzw. Hazard Rules gesprochen. Der regelbasierte Ansatz hinter den Hazard Rules erlaubt jederzeit eine Überprüfung durch einen Experten und ist eindeutig nachvollziehbar. Diese Hazard Rules können manuell oder rechnergestützt erstellt, in einer Datenbank abgelegt und vor der ersten Anwendung überprüft und freigegeben werden. Dieser regelbasierte Ansatz hat neben der Überprüfbarkeit den Vorteil, dass Zusammenhänge erfasst werden können, die durch eine beobachtende und lernende KI nicht erfasst werden würden, da bestimmte Situationen aus Sicherheitsgründen nicht real simuliert werden dürfen und dieses Erfahrungswissen somit nur in den Köpfen der Safety-Experten vorhanden ist. Der regelbasierte Ansatz übersetzt dieses Safety-Erfahrungswissen in programmiertechnisch abbildbare Regeln.

Interoperabilität erfordert Safety-Semantik

Zur Gewährleistung der Interoperabilität zwischen digitalen Zwillingen von Assets unterschiedlicher Hersteller ist für dieses Konzept noch eine einheitliche Safety-Semantik erforderlich. Erste Vereinfachungen heutiger Gefährdungsbezeichnungen, die als Ausgangspunkt für die Entwicklung einer Safety-Semantik verwendet werden können, existieren bereits, siehe bspw. "safety cluster" von TÜV SÜD wie "ungewollte Annäherung" als Ersatz für Kollision, Crash, Zusammenstoß etc.. Im Sinne einer für den Maschinenbau allgemein gültigen Safety-Semantik wird es jedoch als erforderlich angesehen, auf Basis einer noch zu entwickelnden Safety -Ontologie erste Entwürfe einer solchen Semantik systematisch zu entwickeln. Voraussichtlich wird diese Semantik jedoch branchenabhängig zu gestalten sein, um die sprachliche Komplexität in einem beherrschbaren Rahmen zu halten. Möglicherweise ist es sogar für die hier erforderliche Safety-Semantik notwendig, sich von der menschlichen Sprache abzuwenden und eine Semantik analog zum Kraftwerkkennzeichensystem (KKS) zu entwickeln.

Die oben eingeführte Struktur zur Visualisierung eines digitalen Zwillings, siehe Abbildung 2, wurde für die Facetten der aufgeführten Randbedingungen ausgelegt. Dementsprechend wird dem Erfordernis von „Industrie 4.0" dadurch Rechnung getragen, dass nicht nur Safety und der Betrieb adressiert werden, sondern auch die Vertrauenswürdigkeit („Trustworthiness"), in ihrer Gesamtheit bestehend aus Reliability, Resilience, Privacy, Security und Safety. Für eine Detailbewertung einzelner Situationen sind die Maschinenfähigkeiten sowie Profile und die jeweilige Umsetzung („Measures") abgebildet. Der Trust Vector, siehe Abbildung 2, dessen Konzept für eine Erprobung in der ***SmartFactory***^{KL} noch zu bewerten ist und daher hier noch nicht weiter erläutert wird, dient zur Ermöglichung von „Zeit-kritischen Entscheidungen".

5. Use-Case SmartFactory^{KL}

Es wird die Interaktion zwischen einem Menschen und dem Demonstrator der ***SmartFactory***^{KL} Produktionsinsel "Java" betrachtet.

Im betrachteten Szenario wird zwischen verschiedenen Fällen hinsichtlich des Bewegungsstatus des Schlittens des Logistikmoduls unterschieden. In Fall 1 ist der Schlitten nicht in Bewegung. Der ruhende Schlitten stellt somit kein Risiko im Sinne der Safety für die Menschen im Umfeld des Demonstrators dar.

Im zweiten betrachteten Fall ist der Schlitten in Betrieb und somit in Bewegung. Dieser transportiert aktuell beispielsweise ein Produkt zum Handhabungsmodul. Über ein Kamerasystem, das die Werkshalle überwacht, oder behelfsweise über organisatorische Maßnahmen unter Einbeziehung eines digitalen Arbeitsscheinsystems und Zugangsregelungen kann festgestellt werden, wann ein Mensch sich der Anlage nähert, um bestimmte Tätigkeiten auszuführen. Nicht in jedem Fall ist ein Abschalten der Transporteinheit mit Schlittensystem erforderlich. Im Gegenteil, je nach Maschinentyp können bestimmte Inspektionstätigkeiten nur bei Normalbetrieb durchgeführt werden.

Abbildung 4: Physische Darstellung des Szenarios am ***SmartFactory***^{KL} Demonstrator

Aus Safety-Sicht besteht durch die Bewegung des Schlittens bspw. die Gefährdung der Kollision. Das Risiko, das aus Schadensausmaß und Eintrittswahrscheinlichkeit ermittelt wird, wäre in dem Fall, dass sicher kein Mensch in der Nähe des Schlittens ist (d.h. Eintrittswahrscheinlichkeit = „0"), vernachlässigbar.

Durch den Betrieb des Schlittens in Fall 2 ist in dessen digitalem Zwilling die Gefahr „Quetschen" oder „Kollision" aktiv, so dass wie im Whitepaper 2020 beschrieben, der Risk-Reduction-Agent [1] informiert ist, und die Anlage entsprechend überwacht. Weiterhin nehmen wir an, dass ein System mit „Menschen-Gruppe"-Erkennung (Besucher, Werker, Instandhalter) verfügbar ist, welches je nach identifiziertem Menschen-Gruppe entsprechend eine der folgenden Handlungsanweisungen an den Schlitten auslöst, wenn eine Person in den Gefährdungsbereich gelangt:

- ***Wenn der Mensch ein Besucher ist, wird der freizugängliche Schlitten abgeschaltet, also gebremst und in den Ruhemodus versetzt***
  Bei einem Besucher muss unterstellt werden, dass diesem die Gefahren nicht bewusst sind. Durch die Schlittenbewegung bestehen bspw. die Gefährdungen Quetschen und Kollision. Die Schwere (Schadensausmaß) kann berechnet werden, durch die Personenanwesenheit ist der Aspekt Gefährdungsexposition gegeben. Eintritt eines Gefährdungsereignisses und Möglichkeiten zur Vermeidung können bei einem Besucher nicht in ausreichendem Maße unterstellt werden. Man erhält somit ein nicht akzeptables Risiko, so dass der Schlitten abgebremst werden muss.

- ***Wenn der Mensch ein Werker ist, wird der Schlitten verlangsamt („slow down")***
  Bei dem Werker ist dem System in unserem Beispiel nicht bekannt, aus welchem Grund er sich in den Gefährdungsbereich begeben hat. Durch die Anwesenheit ist die Gefährdungsexposition gegeben, jedoch sind dem Werker durch Unterweisungen und durch die tägliche Arbeit die mit der Maschine verbundenen Gefährdungen bekannt, was sich positiv auf die Bewertung von Eintritt eines Gefährdungsereignisses und Vermeidungsmöglichkeit auswirkt. In diesem Fall ist es ausreichend das theoretische Schadensausmaß, hier die Schlittengeschwindigkeit, zu reduzieren, um zu einem akzeptablen situationsspezifischen Risikowert zu gelangen. Die Geschwindigkeitsreduktion beeinträchtigt die Produktivität deutlich geringer als ein kompletter Stillstand.

- ***Wenn der Mensch ein Instandhalter ist, wird Normalbetrieb angeordnet, um eine ordnungsgemäße Inspektion gewährleisten zu können***
  Dem System ist die Tätigkeit des Instandhalters und seine Sondereinweisungen bzw. Trainings bekannt sowie dass hierfür der Normalbetrieb erforderlich ist. Durch die besonderen Trainings des Instandhalters und seine persönlichen Vermeidungsmöglichkeiten k≠ önnte der Eintritt eines Gefährdungsereignisses so weit reduziert werden, dass ein Eingriff in das mögliche Schadensausmaß zum Erreichen eines akzeptablen Restrisikos nicht erforderlich ist.

Sämtliche digitale Zwillinge der relevanten Komponenten des Demonstrators (z.B. Schlitten) sowie Personen verschiedener Rollen und entsprechende Verbindungen sind im Knowledge Graphen entsprechend der Beschreibung im vorherigen Kapitel modelliert. Durch die digitalen Zwillinge sind die Zusammenhänge im Knowledge Graphen eventbasiert mit den physischen Komponenten des Demonstrators verbunden. Somit können entsprechende Handlungsanweisungen getriggert und automatisch durchgeführt werden. Insbesondere bei komplexen Anlagen und Systemen kann dieses Konzept seine Stärken in Form von Zeitersparnis bei nachweislich vollständiger Bewertung ausspielen.

Abbildung 5: Modelliertes Szenario im Knowledge Graphen

6. Ausblick

Im Kontext der Modellerstellung bieten Knowledge Graphen eine Möglichkeit, Safety-bezogenes Wissen strukturiert zu modellieren und dieses über zugehörige digitale Zwillinge, oder im Funktionsumfang erweiterte Verwaltungsschalen unter Verwendung von Safety-Teilmodellen, mit Informationen anzureichern. Somit können zukünftig tendenziell statische Informationen wie z.B. Identifikation eines Assets sowie darüber hinaus auch dynamische Informationen von erheblicher Bedeutung für einen jeweiligen Situationskontext sein (wie z.B. aktuelle Positionierung und Gerätezustand). Safety-Agenten können die dargestellten Ansätze wie digitale Zwillinge mit Knowledge-Graphen zukünftig sowohl als Wissensbasis als auch als standardisierten Zugriffspunkt und Schnittstelle zur Identifikation sowie Beurteilung von Assets und kontextabhängiger Konstellationen verwenden.

Im Hinblick auf die Entwicklung von flexiblen, modularen Fertigungsumgebungen und damit einhergehendem steigenden Autonomiegrad kommt auch Agentensystemen [6] eine stärkere Bedeutung zu, die Merkmale autonomer Systeme [7] erfüllen. Basierend auf [1] bestehen Ansätze, in denen ein Safety-Agent eine Risikobewertung vornimmt und die vorliegenden Modelle und Informationen einbezieht, um mit Anforderungen an sich ändernden Situationen umgehen zu können. Somit kann das Ziel einer verbesserten Bewertung safety-relevanter Konstellationen zur Erhöhung von Flexibilität und Sicherheit erreicht werden.

Literatur

[1] Technologie-Initiative ***SmartFactory*** KL e.V.: Smart Safety Requirements for Digital Machine Representation. Whitepaper SF-3.3: 09/2020, (2020). Online unter: https://smartfactory.de/wp-content/uploads/2020/12/SF_WhitePaper-082020_EN_PRINT-2.pdf.

[2] Technologie-Initiative ***SmartFactory*** KL e.V.: Smart Safety – Sicherheit in modularen Produktionsprozessen. Whitepaper SF-3.2: 04/2019, (2019). Online unter: https://smartfactory.de/wp-content/uploads/2019/03/Whitepaper_AG1_deutsch_042019.pdf.

[3] Technologie-Initiative ***SmartFactory*** KL e.V.: Safety an modularen Maschinen. Whitepaper SF-3.1: 04/2018, (2018). Online unter:https://smartfactory.de/wp-content/uploads/2018/04/SF_WhitePaper_Safety_3-1_DE_XS.pdf.

[4] DIN EN ISO 12100: Sicherheit von Maschinen – allgemeine Gestaltungsgrundsätze - Risikobeurteilung und Risikominderung. Fassung März 2011 (2011).

[5] DIN EN ISO 23125: Werkzeugmaschinen – Sicherheit – Drehmaschinen. Fassung April 2015 (2015).

[6] Ruskowski, M., Herget, A., Hermann, J., Motsch, W., Pahlevannejad, P., Sidoreko, A., Bergweiler, S., David, A., Plociennik, C., Popper, J., Sivalingam, K., Wagner, A.: Production Bots für Production Level 4: Skill-basierte Systeme für die Produktion der Zukunft. atp magazin 62.9 (2020): 62-71.

[7] Wahlster, W. "Künstliche Intelligenz als Grundlage autonomer Systeme." Informatik-Spektrum 40.5 (2017): 409-418.

Versionshistorie
Whitepaper SF-3.4: 05/2022

Herausgegeben von
Technologie-Initiative SmartFactory KL e.V.
Trippstadter Straße 122
67663 Kaiserslautern

T +49 (0)631 20575-3401
F +49 (0)631 20575-3402

Die Technologie-Initiative SmartFactory KL e.V. (***SmartFactory***^{KL}) ist ein gemeinnütziger Verein des öffentlichen Rechts, eingetragen im Vereinsregister Kaiserslautern.

Vereinsregisternummer: VR 2458 Kai

Vorstand
Prof. Dr. Martin Ruskowski (Vorsitzender)
Eric Brabänder, Empolis Information Management GmbH
Andreas Huhmann, HARTING AG & Co. KG
Klaus Stark, Pilz GmbH & Co. KG

Wissenschaftlicher Koordinator
Dr.-Ing. Achim Wagner
T +49 (0)631 20575-5237
M achim.wagner@smartfactory.de

Quellenangabe, Bilder
@WrightStudio - stock.adobe.com
SmartFactory^{KL} / A.Sell